Security

Component Architecture

Revision Date: May 23, 2003

Table of Contents

Section 1 - Background and Decision Tools

Business Direction

Business Direction, which includes Business Influences and Goals and Objectives, forms the foundation of the BEAM process and the DMV's Enterprise Architecture. This foundation is the first step from which all information technology decisions are made and can be traced. Business objectives are common across the DMV enterprise and represent DMV's stated direction for fulfilling the organization's mission. The primary objective of the BEAM process is to develop a flexible, comprehensive, maintainable framework to manage the rapid evolution of technologies that support the business directions of the DMV. This approach will directly link all technologies implemented to specific DMV goals and/or objectives.

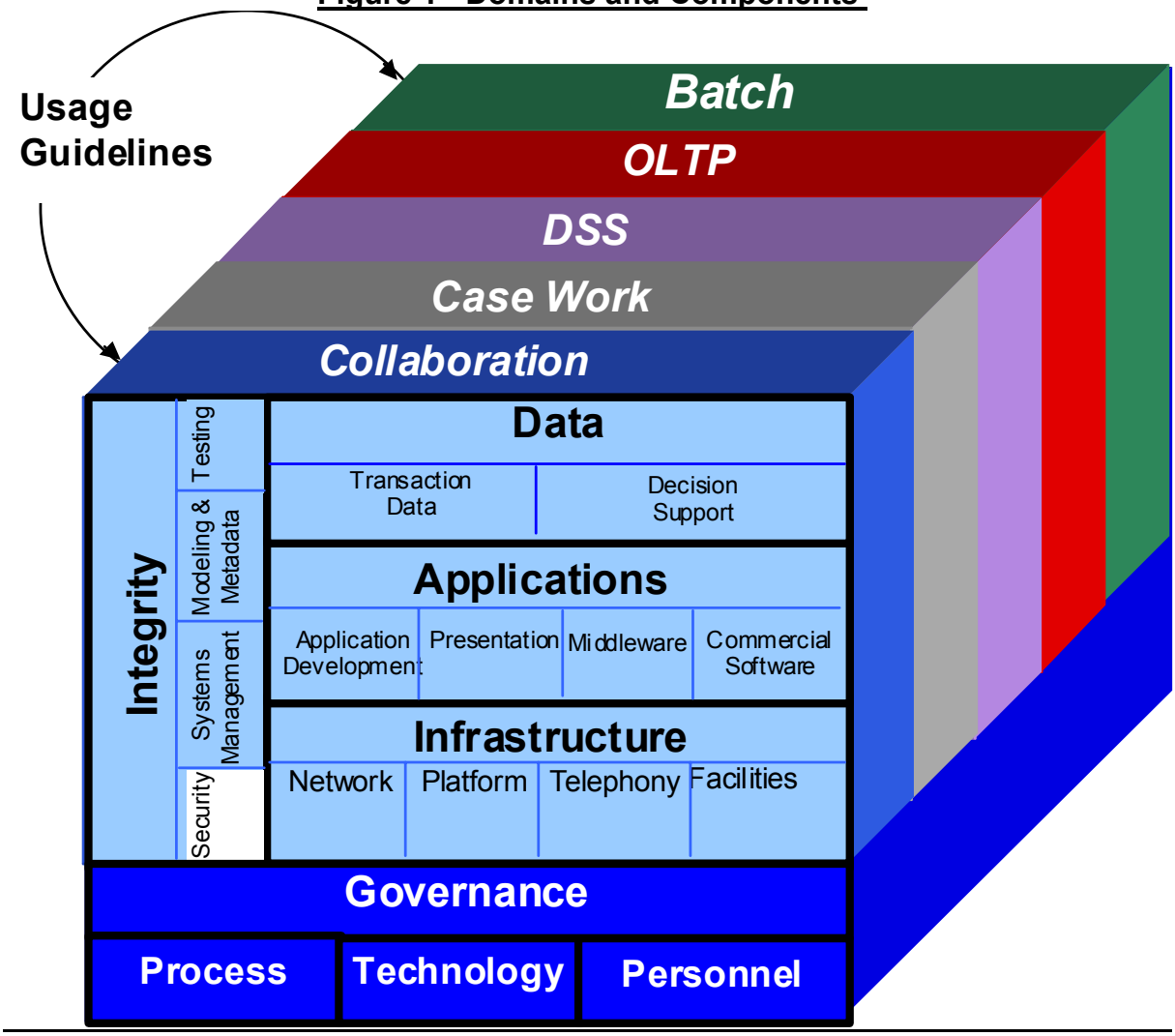
Architecture Requirements

The Architecture Requirements consists of two sections, Information Requirements and Technology Requirements. This is the first step in the BEAM process that begins to focus on specific technologies.

Information Requirements represent the informational needs that are necessary to fulfill DMV's Business Goals and Objectives. Information Requirements bridge the gap between what the Business Goals and Objectives are and what DMV's information systems must deliver to allow management to met these goals and objectives. An individual Information Requirement is typically applicable to more than one Business Objective. Information Requirements are not system or division specific, rather they are related to the information itself. Information delivery refers to the process of delivering information to and from people or groups of people, rather than the input or output of data from databases or applications.

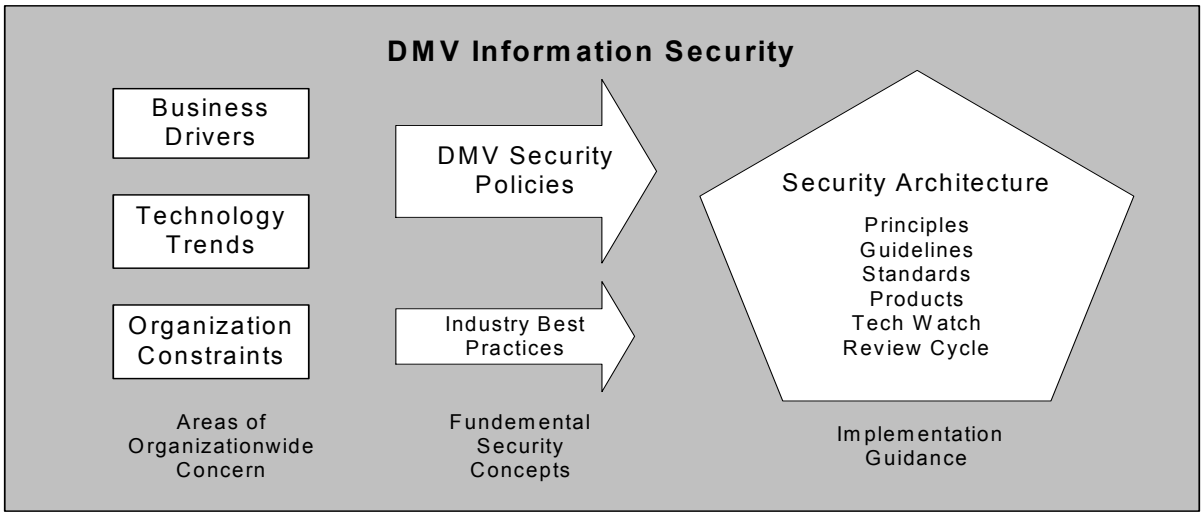
Technology Requirements represent the technologies that satisfy the Information Requirements. In addition, the Technology Requirements feed the DMV Domain Model (Figure 1), which organizes each IT technology into manageable categories called domains, components and Sub-Components. The Technology Requirements detail the specific technologies that satisfy the Information Requirements.

Figure 1 - Domains and Components



Scope

The DMV must provide the speed and flexibility required to deliver technology solutions to meet ever-changing demands. It is imperative that its security environment be optimized for, and integrated with, procedures, tools, and technologies that allow its security management to be extensible, portable, and flexible. The most appropriate toolsets will be those that compliment the standards and products that have been selected for the DMV's current network platforms, network infrastructure, business transactions, and information requirements. As shown in the diagram below, the DMV security architecture is driven according to its business drivers, technology considerations, and most importantly, its security policies.



Security threats can originate from both inside and outside the walls of governmental organizations. External threats can arrive from the Internet or via remote dial-up facilities. A common misconception is of a firewall protecting a company from all external threats. However, a firewall is powerless to stop someone entering a network through an internal computer connected to an unauthorized and unsecured modem. Internal threats arise from employee actions, either intentional or unintentional, misuse of resources, or fraud. Although external threats receive a majority of attention, DMV security policy must also address internal security issues to be effective.

The vision for the security component at the Department of Motor Vehicles is to provide a security architecture that will support its heterogeneous, distributive computing environment, while ensuring a sufficient level of confidentiality, integrity, and availability for its information systems in a cost effective and efficient manner.

The scope of the subjects included in the security architecture at DMV will mirror the core domains recognized within the field of information security; security management, access control, computer security operations, telecommunications and network security, and applications and system development.

> *The Security Component does not address principles, standards, and products regarding physical security of DMV facilities. Those principles can be found in the Facilities Component section of the architecture.*

Conceptual Architecture

The Conceptual Architecture defines the principles and industry-leading best practices that will guide future IT and process decisions. The Conceptual Architecture is derived from DMV's Business Goals, Objectives, Information Requirements and Technology Requirements. Conceptual Architecture Principles (CAPs) are important to the BEAM process because they help ensure that the decisions made later in the Component Architecture development process are consistent.

The following table contains the CAPs for the Security Component.

Security Conceptual Architecture Principles (CAPs)	
Gov Proc 6	Follow a total cost of ownership (TCO) methodology.
Gov-Proc 7	Develop service level agreements (SLA) for all IT services.
Gov-Proc 12	DMV must leverage the BEAM Usage Guidelines when developing and implementing IT systems.
Gov-Tech 1	Design systems (i.e., hardware, software, operating systems, networks) to be robust enough to handle changing business needs.
Gov-Tech 2	Deploy information systems across an N-Tier*, distributed computing environment.
Gov-Tech 3	Design flexibility into the architecture to accommodate continuing business changes and improvements in technology.
Gov-Tech 4	Design DMV systems for scalability and increased functionality.
Gov-Tech 5	Invest in industry leading vendors, best practices, technology standards and products
Infra 1	Centrally manage DMV's IT infrastructure.
Infra 2	Employ communications protocols that span multiple platforms and diverse operating systems.
Infra 3	Regardless of where an employee connects to the infrastructure, once authenticated, provide access to all system resources.
Infra 4	Manage the transport infrastructure, desktop systems and servers with a responsive, measurable set of service level objectives.
Infra 5	Provide an effective integration of DMV's automated voice processing tools and IT systems.
Infra 6	Supporting facilities and services must be engineered and managed to ensure that DMV can respond to new business requirements.
Integrity 1	Centrally manage IT security.
Integrity 2	Ensure that all data stored on servers will be backed-up and recoverable.

Integrity 3	Conduct business without putting the security of DMV's data and information at risk.
Integrity 4	Design for a "single sign-on" user authentication process.
Integrity 5	Design for centralized management of user authorizations for all applications and enterprise services.
Integrity 6	Support a Disaster Recovery Plan that allows resumption of critical processes.

* For a definition of an N-Tier environment, please see the Glossary section of the BEAM intranet site at: http://dmvweb/isd/beam/

Section 2 – BEAM Recommendations

Security Component

The Security Component is composed of the standards, procedures, tools and future-state recommendations, to be used within the BEAM architecture design. This architecture will ensure that DMV data, customer information, servers, networks, applications, and software protected to the degree required to successfully meet DMV business requirements. Specific technology Sub-Components considered within the Security Component include:

Security Management

- Provisioning
- Firewall
- Policy Enforcement & System Hardening
- Incident Response
- Forensic Analysis
- Information Governance
- Awareness & Training
- Cryptography & Key Management

Access Control

- Directory Services
- Authentication
- Authorization
- Remote Access

Computer Security Operations

- Auditing Tools
- Desktop Protection
- Messaging Security
- Anti-Virus

Telecommunications and Network Security

- Intrusion Detection Systems
- Configuration Management

Applications and Systems Development

- Application Authentication and Single sign-on (SSO)
- Application Controls
- Database Controls
- Testing Controls

Security Component Principles

Statements agreed to by the DMV technology professionals that direct the selection, acquisition, deployment and management of the Security Component. The Security Component does not address principles regarding physical security of DMV facilities. Those principles can be found in the Facilities Component document.

#	Security Component Principles
	Security Management
1.	Confidential information in DMV records will be accessed and protected in a manner that ensures its confidentiality, integrity, and availability.
2.	Business owners will be responsible for defining the level of acceptable risk in accordance with DMV information security policies and information governance guidelines. Systems and applications are to be periodically audited to validate risk definitions and verify compliance.
3.	For contained systems with diverse security specifications and acceptable risk definitions, security controls will be implemented to comply with the specifications for the most rigorous protection requirements.
4.	DMV's security system will comply with the State of California's security standards.
5.	The Department of Motor Vehicles will distribute security administration over multiple systems, introducing several layers for a "Defense in Depth" approach.
6.	DMV security policy will be enforced by technological means whenever possible.
7.	All DMV security devices, appliances, and systems will be centrally managed.
8.	Addressable devices within the DMV network that are serving DMV business functions, will be certified as complying with security policy before they can be placed into production.
	Access Control

#	Security Component Principles
9.	The Department of Motor Vehicles will authenticate itself to users for transactions that occur over all Internet/Intranet/Extranet connections (i.e. digital certificates, Secure Socket Layer (SSL), etc.) so external users can verify they are conducting business with the DMV.
10.	Use of authentication tool(s) will be required for verifying visitor credentials (i.e. passwords, user IDs, personal identification numbers (PIN)).
11.	All systems, networks, databases and applications will use standard identification and authentication rules (i.e. syntax, length, expiration, removal).
12.	Private data (includes sensitive data, personal data, confidential data, etc.), transaction information, and emails must be protected when stored on hard drives or removable media by physical access control, passwords, and/or encryption, as appropriate.
13.	The DMV will use an automated, centralized access control system which will allow administration authority to be delegated to appropriate parties, when necessary. Permissions and access rights must be based on standardized groups and/or roles.
14.	Group membership and related roles will be stored in a directory structure accessible by enterprise systems, networks, databases, and applications.
15.	Digital certificates will be used when appropriate to identify and authenticate users.
16.	Both public and private key pairs used for DMV business, will be owned and administered centrally. Key escrow will be used when appropriate to protect the Department.
17.	DMV systems using or accessing private information must record and store enough transaction information to enable forensic analysis.
	Computer Security Operations
18	Use antivirus and other appropriate tools to protect DMV from malicious code (i.e. malware: viruses, worms, trojan horses, etc.).

#	Security Component Principles
19.	Electronic-mail use is a privilege granted by DMV management to facilitate, support, and enhance the user's ability to accomplish approved business functions. DMV's e-mail systems will employ standards and procedures to support secure and confidential communication.
20.	Internet use is a privilege granted by DMV management to facilitate, support and enhance the user's ability to accomplish approved business functions. Information retrieved or downloaded from the Internet shall leverage current technology to ensure its authenticity (i.e. digitally signed).
	Telecommunications and Network Security
21.	Intrusion detection systems (IDS) and\or similar devices will be used in monitoring the DMV network and its critical systems from external or internal threats.
22.	The DMV will implement choke-points (i.e. screening routers, firewalls, choke routers) to create a single-point-of-entry for all users entering the network, and to protect its resources from unauthorized or malicious activity.
23.	DMV managers and employees are accountable for the security of all data resources and records within their areas of responsibility and provide for protection from inadvertent or deliberate alteration, disclosure, destruction, loss or theft.
24.	A Web page that informs internal and external users of DMV's privacy policy must be posted and linked to all entry points.
	Applications and Systems Development
25.	All new or modified applications, including any associated procedures, shall be sufficiently tested to ensure the security and integrity of the information that is processed.

#	Security Component Principles
26.	Each transaction made to a production DMV database that contains confidential or proprietary information must create an audit record. The audit record must be retained for a sufficient period of time to satisfy business needs.
27.	The DMV will instill an end-to-end philosophy regarding security and will ensure that security requirements are considered and integrated as part of the Feasibility Study Report (FSR), as well as compulsory during the entire System Development Lifecycle (SDLC).
28.	A reduced sign-on architecture must be utilized which can support current and future user applications. This system will provide for consolidation of user authentication and authorization information, as well as in simplifying administration.
29.	All security and application designs must support high availability due to the business needs of the organization, through redundancy of communication links, network devices, and backup data, where appropriate.

Security Sub Components

Security Management Sub-Component

Provisioning

Definition

Provisioning is defined as an Enterprise user-access management solution, which provides a vendor and platform-independent exchange of user account / profile information. This information is used to automatically allocate and deploy IT applications, devices, systems, and services to employees, business partners, and customers. Robust provisioning provides centralized management in the creation, deletion, and overall management of user accounts. For example, when a new user starts with the Department, provisioning provides the automatic creation of his/her email account, Firewall ID, Meeting Maker account, mainframe ID, application access, database access, etc. Other benefits of robust provisioning include:

- Faster access to business resources for new employees, contractors, consultants, etc., due to automation across disparate IT systems via a single request
- Ease of administration when adding, modifying, and deleting user accounts
- Elimination of lapses in security that result from a user leaving the Department, without all of their individual accounts not having been deactivated (LAN, internet, email, application-specific, etc.)

Directory services are an essential component in provisioning and are used to store user identities and profile information, group information, administrative attributes, as well as access control parameters and provisioning business rules. This information can be stored in a database and in the case of some products must be stored in a database. The Directory Services Sub-Component identifies the standards and product information in that area

Meta-directories also can play an important role in the provisioning process by matching, mapping, and synchronizing back-end information across the enterprise. Several directory vendors also include meta-directory capability including iPlanet, Novell, and Critical Path.

Current and Future State

Current State	Future State
Variety of accounts, each managed	Centralized management of user accounts

Current State	Future State
by a separate administrator- e.g. mainframe, NT, UNIX, including individual applications	via automated process with Provisioning Software
User data stored on individual application or database server	Lightweight Directory Access Protocol (LDAP) server to be implemented for centralized administration

Guidelines

#	Provisioning Guidelines
1.	Create a single common user profile from which to access user attribute information **Rationale:** • The centralized user information can be easily managed and accessed via a single interface.
2.	To the extent possible the DMV will implement a single provisioning solution **Rationale:** • A single solution will reduce the complexity involved in the environment and will also reduce costs associated with implementation, administration, and integration.

Standards

#	Provisioning Standards
1.	Incorporate LDAP functionality into all new applications developed for DMV **Rationale:** • LDAP has become the standard for storing and accessing profile information. LDAP servers can be fine tuned to provide faster response times than traditional databases due to the amount of static information and minimum amount of write operations required. Many applications and infrastructure now requiring LDAP support.
2.	User data to be stored via directory services **Rationale:** • This will allow DMV to leverage its future architecture, which will be built around a consolidated user database.
3.	The products must support the Security Assertion Markup Language (**SAML**) **Rationale:** • In basic terms, SAML provides the ability for systems to securely exchange authentication, authorization, and attribute information between participating systems. SAML will be a key ingredient in e-Business provisioning and will provide a critical element for supporting the provisioning process involving external users such as vendors, contractors, service providers, and external government agencies.
4.	Workflow capabilities are required to support a complete provisioning process **Rationale:** • Workflow is required to support administrative tasks, such as delegation, multi-person authorization. In addition, workflow is required for multiple processing of provisioning actions. That is, provisioning a service for a new user will require activation of accounts on multiple, disparate systems.

#	Provisioning Standards
5.	Administrative and user interfaces will be web-based **Rationale:** • Web-based interface will provide a ubiquitous, uniform interface across a variety of disparate environments. The web-based interface will also facilitate access from a variety of locations include remote access. Web-based communications can be secured using SSLv3 for encryption of sessions (see Cryptography and Key Management), and a variety of authentication mechanisms can be applied to identify users.
6.	The solution must be event driven **Rationale**: • Event notifications are necessary to drive the provisioning workflow engine and to ensure that critical events are recognized throughout the enterprise in a timely manner.
7.	The solution must provide secure agent technology to interface with key applications, operating systems, and supporting systems. **Rationale:** • The agents are the execution mechanism for the provisioning solution and must interface with the primary applications within the DMV. These agents will be responsible for initiating system changes such as user adds, modifies, and deletes. The agent technology must be developed, implemented and operated in a secure fashion to eliminate vulnerabilities—this requires agent authentication to the provisioning server, and encrypted communications. The interface between the agent and the application must be through standard application programming interfaces.
8.	The solution must have the ability to identify and enforce authoritative data sources **Rationale:** • Applications such as HR are recognized as authoritative data sources for personnel information (i.e. certain attributes associated with an employee). The fact that the HR application is the authoritative data source for these particular attributes must be enforced. That is, only the HR application can add, delete, and modify information in these attributes. This type of functionality is critical for controlling the integrity of information across the enterprise.

Products

#	Provisioning Products
	No Products are currently approved for use at the DMV within this Sub-Component

Tech Watch

Market Consolidation - Although provisioning technology and techniques have been available for years, it is still a fairly immature market and new players have emerged to take a leadership position. The technology and the market leaders are still in the developing stages with expected consolidation of products and vendors.

Products to watch as potentially most suitable for use at the DMV are listed below:

BMC Control-SA - An enterprise wide management solution that provides functionality for automating user management tasks and password synchronization. Product suite supports over 25 platforms and applications including OS/390, Unix, Microsoft Windows NT, email systems, databases and ERP systems. Additionally, Control-SA has functionality to automatically discover and reconcile user identities across the enterprise.

Novell eProvisioning - Provides an entire suite of products that make-up it's provisioning solution. This includes eDirectory, DirXML, iChain and several other Sub-Components. Novell has a great deal of experience in dealing with enterprise-wide provisioning and have a mature product offering in several categories.

Business Layers eProvision Day One - Business Layers is a company focused on delivering solutions for enterprise provisioning. Day One provides the workflow and agent technology to provide a provisioning solution. Day One tightly integrates with an LDAP directory for storing and retrieving user identities and profiles as well as business rules and access control permissions. Furthermore, Day One can handle approvals and escalations, dynamically generate workflow, and generate comprehensive log entries.

IBM Tivoli Identity Manager/Access360 enRole – Access360 enRole is a policy based provisioning solution that interfaces with other enterprise systems to provide a complete security infrastructure. enRole provides the workflow, policy enforcement, and identity management features essential for provisioning. In addition, enRole tightly integrates with Netegrity Siteminder (an access control market leader) to provide policy enforcement on web-based applications. Access 360 boasts the most agents for integration with enterprise applications including MVS, Oracle, Siebel, Windows 2000/NT, RACF, CA-ACF2, and others.

In 2002, IBM bought Access360 and Metamerge. IBM essentially replaced IBM Tivoli Identity Manager (TIM) with Access360 enRole. IBM is also integrating Metamerge (per Gartner - a metadirectory product) with Access360. Gartner believes this product will ultimately become a leading user-provisioning product that tightly integrates with Tivoli Access Manager (a leader in the extranet access management market). The two Tivoli products should provide a leading Identity and Access Management (IAM) product suite solution

Review Cycle

6 months

Firewall

Definition

Firewalls are the core component within a company's Internet Gateway Architecture (IGA). The typical IGA may include three core perimeter devices: a screening router, a dedicated firewall host, and a choke router. The screening router operates on the front, or Internet facing end of the perimeter network, and is used for the initial filtering of external traffic. This is the initial filter for all traffic bound for a company's network. It prevents unauthorized traffic from entering, and therefore reduces the workload for the dedicated firewall machine by performing this task. IGA traffic flows from the screening router, to the firewall, and then to the choke router before entering a company's internal network. A choke router is used to perform a similar function as the screening router, however, it is connected to the company's internal network, and is the "last hop" before traffic is passed into or out of the Gateway. This area between the screening and choke router is defined as the DMZ, or Demilitarized Zone. It is within this area that the firewall is located, along with any services which need to be publicly accessible; Web servers, SMTP, FTP, DNS, etc. The DMZ allows external users access to these devices, while preventing them from having to enter the company's internal network. Placing the servers here also provide a performance benefit for the user, as there is reduced latency due to their location.

"Best practices" for the architecture of an IGA require that all dial-up and extranet users pass through the same authentication process as an outside user, i.e. all traffic will flow through the firewall and will then be directed to the appropriate service or to the internal network, if authorized. These types of connections are typically accomplished via dedicated, high-speed lines that connect to the firewall, or through the use of VPN software.

Firewalls provide security through traffic filtering at a variety of network layers. They can work at the network level, such as a simple packet filter, in which it filters traffic based on an IP address, the direction of traffic, or even based upon the particular destination port. However, the more sophisticated devices, such as stateful inspection firewalls, can now examine the data within a packet up to the application layer. In addition to the simple filtering of network traffic, firewalls are sometimes enhanced to include user authentication, encryption for VPN services, Quality of Service (QoS), traffic shaping, and virus and content screening. More feature-rich firewall products are generally more complex. Complexity can lead to defects in the product, which can then lead to vulnerabilities.

Current and Future State

Current State	Future State

Current State	Future State
Internet Gateway architecture in place, including virus protection and IDS	Maintain current environment.
No internal firewalls utilized within DMV	Internal firewalls will be implemented to protect information-sensitive departments e.g. HR, Finance

Guidelines

#	Firewall Guidelines
1.	All VPN and other remote connectivity will pass through the DMV's Internet Gateway Architecture (IGA) **Rationale:** • All traffic destined for the DMV's LAN\WAN environment, will need to meet the same stringent filtering procedures, as does the traffic that originates from the DMV LAN.
2.	Internal firewalls to be utilized for departments with highly-sensitive information **Rationale:** • The internal firewall will ensure that access to confidential information within certain groups is protected, e.g. Human Resources- salary information, employee reviews, etc.
3.	The Department will utilize a distributed firewall architecture, if necessary, to support geographical constraints **Rationale:** • Companies can utilize distributed firewalls to prevent all traffic from having to enter or leave from the same location. This will reduce unnecessary WAN traffic, as well as improve response time for the user.

#	Firewall Guidelines
4.	The DMV will implement a tiered firewall architecture utilizing independent technologies to provide additional security to the most sensitive components within the environment **Rationale:** • Tiered firewall architectures implement multiple firewalls in series for each layer within the environment. That is, a firewall will be used to protect the De-militarized Zone (DMZ), a separate firewall will be used to protect the middle-tier applications (e.g. application servers) from the DMZ, and a separate firewall will be used to protect the back-end database systems from the middle-tier. The separate firewalls will implement different technologies to add a layer of complexity to increase improve security. Generally, stateful packet inspection firewalls are used for the front-end tiers and application proxy firewalls are used as the back-end to protect sensitive data sources. The number of tiers will depend on the security requirements but should be 2 or 3. Single tier structures are insufficient for the DMV's environment.

Standards

#	Firewall Standards
1.	Firewall products will provide the ability to use of automated software to enable periodic reviews by staff of traffic and incident logs. **Rationale**: • Manual review of firewall logs is time-consuming and resource intensive. Periodic review of logs by security personnel must be incorporated into daily security operations. Automated software can assist with this process, thereby freeing personnel to concentrate on other pro-active management tasks.
2.	The Department's IGA will support various Internet Security controls **Rationale:** • The DMV will employ industry best practices in regard to processes and technology for its IGA e.g. Network Address Translation (NAT), stateful inspection capability, code filtering, centralized administration, and client-side firewall software.

#	Firewall Standards
3.	Application proxy firewalls must be used as the last-line of defense in a tiered firewall architecture. **Rationale:** • Application proxies provide a high degree of security and are ideally suited for protecting a company's mid-tier, providing a second level of protection for web server to application communication, or for application to database\mainframe messaging.
4.	Stateful inspection firewalls can be used as a first-line of defense for the network, as well as security for lower risk environments. **Rationale:** • Stateful packet inspection firewalls provide an excellent degree of protection along with top performance to meet the demands of front-end applications such as web servers. These devices should be implemented as the primary perimeter firewall.
5.	DMV staff working from remote locations will have desktop firewall software installed on their laptops and\or home workstations, or employ firewall hardware appliances. **Rationale:** • Desktop firewall and appliance products protect data located on DMV resources that are sensitive to external attacks or probes- i.e. port scans. Telecommuters which have "always on" connections, such as Digital Subscriber Lines (DSL) or cable modems are most susceptible.
6.	DMV telecommuters or staff working from home will employ firewall hardware appliances to ensure their system's security **Rationale:** • The Department will identify and enforce hardware standards for users' systems that will be accessing the DMV network. This includes any firewall hardware appliances identified as necessary for securing the system.
7.	DMV configuration of telecommuter systems must allow for software metering **Rationale:** • DMV policy requiring the audit ability of user's systems for unauthorized software must be provided by telecommuters' systems as well.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Firewall Products
1.	Checkpoint Firewall-1 Currently in use at the DMV- good logging capability, rich GUI, strong support for third party products via its OPSEC (Open Platform for Security) Alliance
2.	Cisco Pix Firewall Currently in use at TEALE data center. Easy configuration of NAT policies, superior performance when NAT is implemented, and low system maintenance as it runs on its own embedded system, unlike a Unix or Windows NT platform.
3.	Symantec Raptor Firewall Management console integrated into the Microsoft Management Console (MMC), superior data screening- able to parse through the data portion of email messages.

Tech Watch

The firewall market is very mature at this time and the DMV is currently implementing market-leading technology. However, the Department should monitor those products, such as Cisco Pix, which implement hardware, or appliance-based firewall technology. Hardware-based firewalls are becoming increasingly popular and provide good integration capabilities with other security infrastructure: intrusion detection systems (IDS), routers, etc.

Another area the Department will want to consider is the use of client firewall (personal firewall) products for its telecommuters or any other remote users.

Checkpoint VPN-1 SecuRemote- enables local and remote users to securely access resources on corporate networks. Prevents unauthorized access to remote user's computers. Safeguards the network by denying VPN access to insecure clients.

Symantec Desktop Firewall- enables administrators to quickly roll out a highly effective solution. Works intelligently in the background, monitoring both inbound and outbound communications. Optimized for always-on broadband connections such as DSL and cable modems.

Review Cycle

2 years

Policy Enforcement & System Hardening

Definition

Policy enforcement and system hardening refers to the ability for the DMV to monitor compliance with, and enforce policies on systems such as servers and workstations. Where appropriate, this Sub-Component also deals with the management and administration of the DMV's information security policy, while not dealing with the creation and definition of policies. Within the Department of Motor Vehicles, there is a need to clarify the roles between security operations and security regulatory policy. This Sub-Component will defer to the definitions and guidelines established by Information Protection Services (IPS) for the operations and regulatory roles and responsibilities. Furthermore, this Sub-Component will address only the requirements dealing with systems, and the need to harden systems against intrusion, as well as monitor for policy enforcement.

In order to automate and scale the ability of a Security Operations group to meet the DMV's requirements, the use of technology in the hardening and policy enforcement process is required. Technology will be considered in the following areas:

1. System testing tools and procedures.
2. System hardening scripts and procedures.
3. Secure operating system implementation.
4. Vulnerability scanning tools.
5. Enterprise security management tools such as host based monitors.

In addition to the above methods for system hardening and policy enforcement, process and procedure guidelines will be required to support the tools and ensure effective deployment of the tools. As with Intrusion Detection Systems, it is impossible to completely harden and enforce policies on all systems, as this would have a detrimental affect on the DMV's ability to conduct business. Therefore, the effort and comprehensiveness of the hardening and enforcement must be balanced against the risks present in the environment. The tools that are employed should not unreasonably impact the ability and performance of individual systems or the network.

Automation of policy enforcement will introduce new vulnerabilities and exposures into the DMV unless due care is applied and proper controls ("checks and balances") are implemented. Therefore, additional process and technology considerations will be

required in the architecture, including workflow (and approval) functionality to mitigate the risks introduced through automation.

Current and Future State

Current State	Future State
Security operations currently performed by Network Infrastructure Support, a group originally responsible for product testing and development. Performing these tasks within security is impacting its ability to perform its initial responsibilities.	Dedicated security operations team to be developed that is security certified and sufficiently staffed.
Security enforcement is not in place at DMV at this time. The Information Protection Services (IPS) group is performing more of a consultative role at this time.	New security operations team will be responsible for the monitoring and enforcement of DMV security policies.

Guidelines

#	Policy Enforcement & System Hardening Guidelines
1.	A centralized and dedicated security operations group will be utilized for policy enforcement **Rationale:** • Centralized operations will be required to provide a sufficient incident response capability in dealing with security incidents e.g. easier identification of security alerts, coordination in communicating with employees, enforcement of standards.
2.	The security operations team will be separate from all DMV development and daily operations groups **Rationale**: • To adhere to the security principle of “separation of duties,” the security operations team will not be involved in network operations or development tasks, preventing a single individual from compromising a system’s control features.

#	Policy Enforcement & System Hardening Guidelines
3.	All security infrastructure and security-related software will be configured to maximize its functionality **Rationale**: • With the rollout of new security products within the DMV, the security operations group will ensure that the full capability of each security product is implemented, if aligned with current strategies.

Standards

#	Policy Enforcement & System Hardening Standards
1.	Vulnerability scanning tools will be utilized
2.	Host-based policy enforcement tools will be employed at the DMV
3.	Workflow is to be considered a required function of policy enforcement tools used in mitigating risks associated with automation
4.	Enterprise security management tools will be centrally managed with distributed capabilities for administration and monitoring
5.	Enterprise security management tools and agents will support SNMP

Products

#	Policy Enforcement & system Hardening Products
1.	Nessus Security Scanner Freeware product, currently in use at the DMV. Provides powerful, up-to-date, and easy to use remote security scanner. Has a client\server architecture. The server performs the attacks, and a client, which is the front-end. You can run the server and the client on different systems. Uses several clients: one for X11, one for Win32 and one written in Java.

Tech Watch

Products to watch as potentially most suitable for use at the DMV are listed below:

BMC Control SA - Enterprise-wide security standards, pre-defined rules for fully automating the user set-up process, transactions monitored through completion

Pentasafe VigilEnt Policy Center - Customizable employee/user web interface which allows users to log on and review, publish, and distribute policies; email alerts sent to users, partners, etc. when new policy is published, online testing for validating users understanding of the policies.

Tivoli SecureWay Security Manager - Ensures the consistent configuration of access rights on operating systems from desktops to mainframes, integrates with Tivoli Enterprise Console for centralized security event management.

Symantec Enterprise Security Manager - Automates the discovery of security vulnerabilities and deviations from the security policy. Allow administrators to create security baselines for every system on the network and measure performance. Used for remote administration and management of servers, workstations, routers, hubs, applications, and databases for security policy enforcement.

For products related to this area, please refer to the “Firewall” and the “Intrusion Detection Systems” Sub-Components.

Review Cycle

6 months

Incident Response

Definition

Incident Response deals with the procedures used by DMV to handle potential threats. This process consists of procedures that allow the organization to react to security events and in controlling the threats. The incidents can range from corrupted data files, to viruses, to natural disasters. Some of these mishaps can be fixed through standard operating procedures. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe events, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan (Refer to the Disaster Recovery Planning Systems within the Systems Management Component for the standards and guidelines in that area). Other damaging events result from deliberate malicious technical activity (e.g., the creation of viruses or system hacking). A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It is used to broadly refer to those incidents resulting from deliberate malicious technical activity. It can also refer to those incidents that, without a technical expert response, could result in severe damage.

Incident handling is closely related to contingency planning as well as support and operations. An incident handling capability may be viewed as a component of contingency planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats. The benefits of Incident Response include:

1. The capability of containing and repairing damage from incidents, and in preventing future damage
2. An incident handling capability will allow organizations to collect threat data that may be useful in their risk assessment and safeguard selection processes (e.g., in designing new systems)
3. Organizations often find that an incident handling capability enhances internal communications and the readiness of the organization to respond to any type of incident, not just computer security incidents
4. The organization's training process can also benefit from incident handling experiences. Based on incidents reported, training personnel will have a better understanding of users' knowledge of security issues.

Current and Future State

Current State	Future State
DMV's Computer Security Information Response Team (CSIRT) is currently developing an Incident Response plan	Continue existing development of a formal method for communication and management of security incidents
DMV consists of various groups, each with separate functions	Incident response plans must take into account each group's needs, possibly developing multiple plans

Guidelines

#	Incident Response Guidelines
1.	Reaction to potential threats must be swift for Incident Response procedures to be effective **Rationale:** • The spread of potential threats must by limited- the sooner the process is enacted, the sooner the risks can be mitigated.
2.	Notification procedures must be in place to notify the proper personnel **Rationale:** • Notification procedures must be in place so the proper personnel, who have the knowledge to mitigate the risk, can handle threats.
3.	If possible, potential threats should be quarantined. **Rationale**: • The spread threats can be the most damaging to an organization. Some malicious viruses or code are designed to utilized network resources to spread.

#	Incident Response Guidelines
4.	The Incident Response plan will be developed according to the current DMV workflow and include the Internet emergency response team- the Computer Emergency Response Team (CERT) as part of the response procedures. **Rationale**: • The response plan will be based around the established procedures for conducting DMV business. The plan will also implement a centralized reporting structure, for tracking purposes.

Standards

#	Incident Response Standards
1.	Systems containing sensitive data must provide audit logs and trails that can be used for analyzing incidents **Rationale**: • Without sufficient information from audit logs, the organization cannot learn from the incidents so that they do not occur again.
2.	Incident Response procedures will integrate with problem management software (e.g. Remedy AR) for alerts **Rationale**: • The DMV will be able to leverage its existing investment in Remedy for sending alerts to administrators and end users.
3.	The Incident Response systems will support priority-based, cascading notifications to a variety of media including e-mail and pagers **Rationale**: • Priority notifications are required to notify the correct individuals and in the order determined. Cascading notifications are required to notify secondary/backup individuals in the event that primary contacts do not respond. Notifications via a variety of media must be supported (either in series or in parallel) to support the tools used within the environment and by support individuals.

Products

#	Incident Response Products
	No Products are currently approved for use at the DMV within this Sub-Component

Tech Watch

Honeypot Networks - Follow the industry practice of employing the use of honeypot networks to misdirect attackers, which is an emerging trend in enterprise information security, for potential adoption at the DMV. Security administrators set up a honeypot network by designing a section of an enterprise's network to make it attractive to intruders. This section will contain false information that appears to be important, for example, application source code or future marketing plans. Once an intruder enters this area — which no authorized user would have reason to enter — the system automatically alerts security staff, who begin tracking the intruder's activities and may even feed him disinformation for the purpose of learning more about his identity and location.

Products to watch as potentially most suitable for use at the DMV in the area of Incident Response are listed below:

BMC Control SA - Enterprise-wide security management provided from a central point of control, providing centralized management capabilities of users, resource access and security policies.

Pentasafe VigilEnt Security Manager - Manages multiple heterogeneous systems from a central point of control, provides a centralized, cross-platform tool for enterprise-wide auditing and security management.

Peregrine Corporation Action Request (AR) - Remedy provides an incident tracking, reporting and notification solution.

Resource Technologies' Mantrap - Extends the Honeypot concept by creating an entire network of deception hosts that lure the attacker away from production systems. Provides organizations with an additional layer of defense that supplements the current abilities of current security solutions, such as firewalls or intrusion detection systems. Useful in the defense against attacks from both internal and external sources.

Review Cycle

6 months

Forensic Analysis

Definition

Computer forensics is the use of science or technology in the investigation and establishment of facts or evidence relating to information security that could be used in a court of law. Information must be collected without contaminating or altering any of the gathered information. A time-based reconstruction of the compromise or attack is created from the forensic analysis and answers question such as, what compromise occurred, when did this occur, and how did the events unfold. This information may or may not lead to action by the Department, but without proper control procedures in place, the organization will not be able to substantiate and support the evidence. Without the following minimum standards, the analysis and evidence may not be considered reliable enough for a court of law, if prosecution is required.

The use of forensic tools will depend on the incident, defined procedures, business drivers, and the forensic teams analysis & judgment on the application of best practices. The uses of forensic analysis techniques are often disruptive to normal business operations due to its methodology and legal requirements. One example of this includes the quarantine of all data and IT infrastructure that may have been involved in the computer crime. Strict adherence to this rule is necessary so that the evidence may be introduced into a court of law, if necessary. Therefore, a business decision would need to be made by senior management as to whether the situation warrants a forensics investigation or not, based upon a cost-benefit analysis.

Current and Future State

Current State	Future State
Limited capability of forensic analysis via the Disk Analysis Retrieval Team (DART)	Computer forensics group to improve its response time to meet DMV demands. A dedicated forensics group will be established and will become more closely aligned with the Department's staff

Guidelines

#	Forensic Analysis Guidelines
1.	Identify a team within the DMV responsible for Computer Forensics **Rationale**: • A single team must be identified with responsibility to develop the computer forensic capabilities within the DMV to assure best practice implementation and execution, as well as maintaining a consistent methodology. A single team will be essential for developing standards regarding the methodology to be followed, as well as training and awareness for all appropriate users, and to create a forensics lab that is complete with all current forensic technologies.
2.	Sterilize all media **Rationale**: • The media that original data is being copied to must be free of all data so that valid bit-by-bit data can be transferred and properly analyzed.
3.	Preserve original media **Rationale**: • Original media must remain unaltered in the event that additional analysis must be performed. Analysis should be conducted on true bit image copies.
4.	Analyze true bit image copies only **Rationale**: • True bit image copies are the only exact copies that will give accurate enough results to be analyzed.
5.	Maintain a strict chain of custody **Rationale**: The media to be analyzed must be controlled by the proper personnel to ensure the integrity of the information. This is vital that that information may be used as evidence in a court of law and must not be altered.

#	Forensic Analysis Guidelines
6.	Develop and store complete documentation on the processes and results of each analysis **Rationale**: • Without thorough documentation, analysis will not be complete and may be inaccurate. The analysis documentation should be thorough including date/time stamps, individuals involved, processes, findings, theories, decision factors, and constraints.
7.	Secure all media, analysis, reports, and additional data pertinent to the investigation. **Rationale**: • The media, analysis, reports, and pertinent data are critical elements in the investigation of an incident and must be secured to protect the integrity, confidentiality, and availability of the material in the event that the material may be used in further action.
8.	Forensic analysis tools will be collected and utilized by the DMV to address the forensic requirements of the DMV's key systems **Rationale**: • Tools must be acquired to perform collection and analysis on a wide variety of media and data structures, including workstations, mainframes, personal digital assistants (PDA), ASCII, EBCDIC, Unicode, and Binary.

Standards

#	Forensic Analysis Standards
1.	Disk Analysis tools are required **Rationale:** • Disk analysis is a critical element in forensics and the tools must have the ability to analyze physical and logical disk media. This includes the ability to recognize disk partitions and volumes, including those that maybe hidden.

#	Forensic Analysis Standards
2.	The media imaging tools must provide the ability for a bit-by-bit copy. **Rationale**: • Imaging tools will ensure that evidence is protected and preserved. Analysis must only take place on backup images and not on the original media/data.
3.	Basic decryption and password cracking tools will be required for analysis of protected information **Rationale**: • Basic decryption and password cracking tools are available on the market for breaking simple encryption algorithms or performing brute force password attacks. For example, this includes the ability to open protected Zip files or password protected Microsoft Office files. In addition, password crackers are available for passwords stored in various operating systems and applications.
4.	Keyed-Hash and/or digital signature tools are necessary for assuring the integrity of information **Rationale**: • Keyed hash techniques provide the ability to verify the integrity of information that is undergoing forensic investigation.
5.	File search utilities will be an essential component of the forensic toolkit **Rationale**: • File searching is an everyday task of forensic analysis. This utility will be required to search a variety of media and a variety of file formats. Binary searches will also be required.
6.	The DMV's forensic toolkit will consist of a good quality (at least a 2.1 mega-pixel, 3x optical zoom, and macro lens) digital camera. **Rationale**: • The digital camera will be an essential tool for capturing visual evidence of the scene of an incident. A good quality digital image will be required to provide sufficient image clarity and detail.

#	Forensic Analysis Standards
7.	The DMV will purchase and install an excellent quality large capacity safe **Rationale**: • The safe will be required to provide physical safeguards for investigative information and/or evidence.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Forensic Analysis Products
1.	dtSearch dtSearch provides a powerful and flexible search engine that is an essential ingredient in forensic investigations and the analysis of data. dtSearch can search a variety of files including text, PDF, HTML,
2.	WINHEX This is an inexpensive but valuable utility for performing forensic analysis on a variety of files including ASCII, EBCDIC, and Binary. WINHEX has been enhanced in recent versions to include valuable forensic functionality including data integrity checks, disk imaging, disk editing, disk wiping, partition recovery, data interpretation, and bookmarking.
3.	Symantec Norton Utilities & Ghost Norton Utilities provides a variety of disk and file utilities that will be handy during forensic analysis. Ghost provides disk-imaging functionality.

Tech Watch

A best practice with computer forensic products is to acquire a “tool chest” that contains a variety of best-of-breed forensic tools. There are a variety of forensic tools available in the market, with each product offering unique benefits. Although overlaps exist in many of the products, there will be specific features within each product that provide the best-of-breed tool that meets the needs of the analysis being conducted. It may therefore be necessary to purchase several products to ensure that the appropriate tool or tools are at hand when required. The cost of these products is fairly low (from a few hundred to a few thousand dollars) and can be justified in a short period of time with just one successful investigation of an incident.

Analysis of mainframe files and logs can take place on workstations equipped to handle file/log images. A variety of tools have been listed that will work with data in the EBCDIC format.

Products to watch as potentially most suitable for use at the DMV in the area of Intrusion Detection are listed below (in addition to products listed below, there are several companies available in the market that can provide forensic services (such as data recovery, disk recovery, and analysis) on both workstation and mainframe systems):

New Technologies Inc. (NTI) - Has been in the computer forensic business for over 10 years and provides a suite of forensic utilities designed for law enforcement, government, and commercial customers. Certain utilities are only licensed to law enforcement organizations. The tools provide both physical and logical analysis of a variety of media and data structures. This is a comprehensive suite that provides valuable utilities for finding, searching, filtering, analyzing and cataloging data on a variety of disk media. The tools are primarily focused on Microsoft platforms, but file based utilities can be used for any type text formatted information. In addition to the utilities, NTI provides forensic training.

Guidance Software EnCase & FastBloc - Provides a robust set of forensic tools (software & hardware) for analyzing a variety of media using several techniques, including non-invasive methods. EnCase also provides a useful MS Windows graphical interface for analyzing information and media images with several inclusive features that are beneficial to the analysis process. The tools can be used for several Operating System platforms including Microsoft, Linux, and Unix. Guidance also provides forensic training.

Columbia Data Products Snapback - Provides solutions designed to create a “True Image Backup” of hard drive media. An exact byte-by-byte copy of the hard drive **media can take place while the server continues operations.**

Digital Intelligence - Provides a suite of computer forensic platforms (F.R.E.D. series) that consist of a variety of hardware and software tools. The platforms provide the computer and hardware components essential in a forensic lab, along with support software for disk imaging, partitioning, wiping, and analysis. The Digital Intelligence platforms would be used in conjunction with other physical and logical forensic tools.

Review Cycle

6 months

Information Governance

Definition

Information governance address the question, “Who is responsible for this data?” Of course, on a basic level the answer is simple: computer security is the responsibility of everyone who can affect the security of a computer system. However, the specific duties and responsibilities of various individuals and organizational entities vary considerably. Information governance gives the authority to administer data to the person or group responsible for its use. This also allows the owner of the data to be accountable for any incidents that affect access to the information.

By defining the governance over information, the organization establishes a computer security program that includes overall program goals, objectives, and priorities in order to support the mission of the organization.

Current and Future State

Current State	Future State
An established Information Security Office is currently in place.	Develop security a policy that outlines data governance for the respective business organizations.
No procedure for managing the information lifecycle.	Develop policy and an oversight team to handle this function.
Business units are aware of the sensitivity of their data.	Maintain current environment.

Guidelines

#	Information Governance Guidelines
1.	Establishment of information governance policies. **Rationale**: • The policies will guide organization with information security and be a published document for all personnel to follow

#	Information Governance Guidelines
2.	Define and classify data assets and Data Resource Managers (DRM) **Rationale**: • This allows business units to be aware of their data. Although each unit may not be directly responsible for securing their data, they will have to identify the necessary level of security.

Standards

#	Information Governance Standards
	None

Products

#	Information Governance Products
	None

Tech Watch

N/A

Review Cycle

3 years

Awareness & Training

Definition

The purpose of computer security awareness, training, and education is to enhance security by:

1. Improving awareness of the need to protect system resources;
2. Developing skills and knowledge so computer users can perform their jobs more securely; and
3. Building in-depth knowledge, as needed, to design, implement, or operate security programs for DMV organizations and systems.

Making computer system users aware of their security responsibilities and teaching them correct practices, helps users to change their behavior. It also supports individual accountability, which is one of the most important ways to improve computer security. Without knowing the necessary security measures (and to how to use them), users cannot be truly accountable for their actions. The importance of this training is emphasized in the U.S. Computer Security Act of 1987, which requires training for those individuals involved with the management, use, and operation of federal computer systems.

Training teaches people the skills that will enable them to perform their jobs more securely. This includes teaching people what they should do and how they should (or can) do it. Training can address many levels, from basic security practices to more advanced or specialized skills. It can be specific to one computer system or generic enough to address all systems.

Current and Future State

Current State	Future State
Users are given periodic security updates via email, information pamphlets, newsletters, and certification programs.	Continue with comprehensive awareness program, utilizing multimedia updates.
No current policy regarding security awareness for consultants, contractors, students, or other temporary staff.	All new and existing users to sign HR document specifying that they have read and will comply with the DMV security policy regarding computer usage.

Guidelines

#	Awareness and Training Guidelines
1.	Make users accountable for their actions pertaining to information security **Rationale**: • Both the dissemination and the enforcement of policy are critical issues that are implemented and strengthened through training programs. Employees cannot be expected to follow policies and procedures of which they are unaware. In addition, enforcing penalties may be difficult if users can claim ignorance when caught doing something wrong.
2.	Customize training according to the audience **Rationale**: • Not all audiences will have the same issues or concerns; therefore segmentation will allow information to be transferred more effectively. Separating audiences based on job title, job task, or level of knowledge will help get the correct information to the correct audience.
3.	Motivate Management and Employees to comply with security policies. **Rationale**: • To successfully implement an awareness and training program, it is important to gain the support of management and employees. Consideration should be given to using motivational techniques to show management and employees how their participation in a security awareness program will benefit the organization.
4.	Utilize multiple methods to establish security awareness and training, including: **Rationale**: • "All-hands" meeting**s -** Other departments (such as Human Resources or the Legal Department) will conduct meetings for all employees to cover such topics as sexual harassment, drug abuse awareness, workplace conduct, etc. This is an excellent opportunity for you to collaborate with these other departments to incorporate the Department's information security message into part of the presentation. • Intranet Portal - Excellent place to post the security policy, as well as a number of security awareness features. For this method to be effective, the content will need to be changed regularly. Awareness technique currently in use at the DMV. • Memos - Security memos printed on paycheck stubs, email updates, screen savers, login scripts, and hardcopy memos sent through inter-office mail, provide high-visibility opportunities. Email memos and screen savers currently in use by Information Protection Services.

#	Awareness and Training Guidelines
	• Login Message / Warning - The Login Message should comply with DMV policy and provide a warning that the computer system is for authorized use only. These messages should be mandatory on all systems that require a user or resource to login.

Standards

#	Awareness and Training Standards
	None

Products

#	Awareness and Training Products
	No products are currently approved for use at the DMV within this Sub-Component

.

Tech Watch

Evaluate the use of videos from organizations such as the Computer Security Institute. Videos are one of the most effective, but also among the most expensive, forms of communication. Videos can be an excellent training tool if they can be reused numerous times, such as for new-employee orientation.

Review Cycle

6 months

Cryptography and Key Management

Definition

The use of cryptography for providing authentication, integrity, and non-repudiation for electronic transactions, has become a de-facto standard for eCommerce activities, which can be leveraged within the world of eGov business. Public keys are electronic files, which are exchanged or submitted as proof of identity for a particular machine and\or user. These keys are part of a larger system, PKI- Public Key Infrastructure, which is the basis of Internet and extranet user authentication. The certificate binds a public key to a specific user workstation. When communicating, each party exchanges certificates, or keys, which are used to establish an encrypted channel for communication.

PKI vendors generally fall into two categories: those providing software products that let an organization become a CA (Certificate Authority) and distribute certificates, and those acting as a CA service bureau, distributing and managing certificates on behalf of users and enterprises. There is some concern within the DMV regarding vendors that fall into the second category. The concerns are related to the abdication of duties and responsibilities for identifying and verifying the identity of employees and partner agencies requiring digital certificates.

One of the core security principles accomplished through cryptography is “non-repudiation.” This feature is the assurance that a person’s actions are properly attributed and cannot be denied by the party whom initiated the action. This is done with strong audit methods, with entities whose identities have been strongly authenticated. Digital signatures have the characteristic that, if properly implemented, can be used to provide non-repudiation.

Current and Future State

Current State	Future State
No formal adoption of cryptography tools in place. Limited use of digital certificates; DMV field offices, court documentation via the Internet, and web servers.	Use of digital certificates and signatures will be integrated into the DMV environment as a security control.

Guidelines

#	Cryptography and Key Management Guidelines
1.	Digital certificates will be used by the DMV to perform two-way authentication in its communication with other agencies and customers. **Rationale**: • Users will be able to verify that they are doing business with the DMV. Also, this technology is necessary for when there is more than financial implications at stake, such as the submission of regulatory documents.
2.	Non-repudiation of actions will be facilitated through the use of digital signatures. **Rationale**: • Digital signatures are a legally enforceable method for assurance in data transactions and can be used on any type of communication between business contacts, e.g. EDI, e-mail.
3.	DMV will employ at least two-factor authentication for all remote users connecting to DMV resources **Rationale**: • \Due to insecure nature of dial-up connections, employees will utilize VPN and other standard technology for authentication and confidentiality purposes. For example, a username\password or PIN will be combined with a smart card to provide strong, two-factor authentication.
4.	DMV will develop a Certificate Practice Statement (CPS) & Certificate Policies (CP) in compliance with the California Digital Signature Legislations as adopted by the Secretary of State. **Rationale**: • The DMV will ensure compliance with accepted best practices in the design, implementation, and operation of Certificate Authorities, and the use of digital certificates. The CPS and CP's are critical elements for documenting the standards implemented and followed by the DMV for operation of a Certificate Authority and for the use of digital certificates.
5.	The use of cryptography within the DMV must account for the performance requirements of the systems, and the use of hardware accelerators must be considered where performance could be degraded beyond acceptable levels

#	Cryptography and Key Management Guidelines
	Rationale: • Performance is a critical factor within the DMV environment, where sub-second response times have been established for mission critical systems. Degradation of performance beyond acceptable limits will negatively impact the business, therefore cryptographic accelerators must be considered.

Standards

#	Cryptography and Key Management Standards
1.	The DMV will utilize encryption for all sensitive data that travels over public networks. **Rationale**: • DMV communication from remote offices to TEALE or other central IT facilities, will need to ensure the confidentiality and integrity of information through the use of current encryption technologies, i.e. SSL/TLS, IPSec, SSH, PPTP.
2.	The DMV will utilize public key cryptography to securely exchange symmetric keys **Rationale**: • Public key (asymmetric) cryptography provides an industry standard, secure, method for authenticating two parties and securely exchanging symmetric key information. This exchange is necessary for protocols such as SSLv3 and is used extensively for encrypting and exchanging secure documents (i.e. where the symmetric key is used to encrypt the document, and the public key cryptography is used to securely exchange the symmetric key with parties that are authorized to view the document).
3.	The DMV will utilize the RSA, DSA, Diffie-Hellman, and Elliptical Curve public key cryptographic (PKC) algorithms with sufficient key strength where applicable **Rationale**: • These are industry accepted and generally proven algorithms for public key cryptography. Acceptable key lengths will vary depending on the algorithm and the specific use.

#	Cryptography and Key Management Standards
4.	The DMV will use X.509 digital certificates **Rationale**: • X.509 has become the de facto standard for digital certificates. The digital certificates can perform mutual authentication between the server and the user, before the secret keys are shared, increasing the integrity of the certification process.
5.	The DMV will implement symmetric cryptography that utilizes the recently ratified Advanced Encryption System (AES). **Rationale**: • This is the replacement algorithm for DES and has been designed for longer cryptographic keys (256 bit versus 56 bit). The 56bit key used in the DES algorithm is no longer sufficient for protecting the confidentiality of information. With the advancement of computing technology, it is essential to utilize strong cryptographic algorithms and longer key lengths.
6.	For secure web-based communications, the DMV will use SSLv3 with at least 128bit encryption, and with mutual authentication in situations requiring strong authentication **Rationale**: • SSLv3 has become the defacto standard for secure web-based communication. Although SSLv3's primary role is to secure HTTP traffic (i.e. HTTPS), the protocol has been adapted for use with other network protocols including LDAP, POP, and SMTP. To mitigate the risks associated with man-in-the-middle attacks, the DMV will utilize mutual authentication for highly sensitive communications—or those communications requiring strong authentication. Typically, SSLv3 implementations only require the server to authenticate itself to the client (e.g. browser) using a digital certificate and public key cryptography. Mutual authentication requires both the client and server to authenticate using digital certificates and public key cryptography.
7.	The DMV will implement revocation checking (CRLv2 and OCSP) for all production systems relying on digital certificates **Rationale**: • Revocation checking is essential to determine the current validity of a digital certificate. This is accomplished by checking a revocation list residing in an LDAP repository, or using the OCSP protocol for making a real-time check. The DMV must ensure that any OCSP implementation is performing a real-time verification check directly to the Certificate Authority database, rather than using a responder relying on an aged CRL list—this provides assurances on the near real-time validity of the digital certificate.

#	Cryptography and Key Management Standards
8.	The DMV will implement public key cryptography tools that comply with the IETF PKIX proposed standards **Rationale**: • PKIX is being adopted as the standard set of protocols and data structures for communicating and exchanging information in public key environments. This includes a proposed standard set of protocols for communication between clients and certificate authorities, and between certificate authorities for such events as certificate issuance and cross certification. PKIX also defines data structures and elements, such as the mandatory and optional data elements in an X.509 certificate.
9.	The DMV will implement a solution that supports key escrow and key recovery for cryptographic keys that are used to encrypt data **Rationale**: • Key escrow and key recovery are critical elements for ensuring that the DMV can recover information in situations where the original keying material has been lost, corrupted, or purposely destroyed. Only keys used for encrypting information must be escrowed. Keys used for digital signatures and non-repudiation cannot be escrowed.
10.	The DMV will only implement an approved third party service Certificate Authority (and Registration Authority) as appropriate for the business and in compliance with the DMV Certificate Practice Statement and Certificate Policies. **Rationale**: • The certificate authority (CA) and registration authority (RA) will be required to register new users, issue digital certificates, and revoke or suspend certificates.
11.	The DMV can function as an in-house Certificate Authority (CA) only upon meeting the requirements provided by California Digital Signature Legislations, obtaining certification, and complying with the Department's Certificate Practice Statement and Certificate Policies. **Rationale**: • The DMV will be required to register new users, issue digital certificates, and revoke or suspend certificates upon functioning as a CA.

#	Cryptography and Key Management Standards
12.	The DMV will employ Hardware Security Modules (HSM) compliant with at least FIPS 140-1 Level 3 for sensitive keying material **Rationale**: • HSM's are hardware devices used to protect sensitive cryptographic keys. HSM's are designed with varying degrees of security to protect and backup the keying material including the ability to zero-ize the keys if the device is compromised. HSM's also provide cryptographic acceleration by offloading the cryptographic processing to the hardware device.
13.	The DMV will deploy Smartcards or other cryptographic tokens to users to provide strong authentication with the use of digital certificates **Rationale**: • Strong authentication generally requires 2-factor authentication such as something you know and something you have. Smartcards can provide 2-factor authentication by storing digital certificates and PKC keying material on a separate physical card or token. This information is protected by the user's PIN.
14.	The DMV will deploy cryptographic solutions that are compliant with Public Key Cryptography Standards (PKCS) **Rationale**: • PKCS defines generally accepted standards for use in PKC environments including RSA public key use, certificate requests, and file storage of PKC material. These standards include but are not limited to: PKCS#1, #7, #10, #11, #12, and #15.
15.	The DMV will use the IPSec protocol for virtual private networking (VPN) security **Rationale**: • IPSec is the defacto standard for securing VPN's, and provides protocols for authentication, encryption, and integrity checking.

Products

#	Cryptography and Key Management Products
	No products are currently approved for use at the DMV within this Sub-Component.

Tech Watch

Products to watch as potentially most suitable for use at the DMV are listed below:

Entrust - Provides an entire suite of mature products (including Authority and Entelligence) designed specifically for the enterprise. This suite includes both server side and client side software components. Used within the enterprise, Entrust provides and excellent platform for managing the entire lifecycle of cryptographic keys, including simplified key escrow and key recovery. Entrust also provides web-based components, a third party certificate authority service, and a comprehensive development toolkit.

iPlanet Certificate Management System (CMS) - iPlanet CMS is a highly scalable and flexible PKI solution that has been designed for companies to deploy their own Certificate Authority to support millions of users. The solution supports certificate requests from clients (including VPN), servers, and network devices such as routers. CMS provides key escrow & recovery for long-term storage of encryption keys. The management console uses the standard web browsers for ease of administration from almost any location, and the back-end CA/RA is highly configurable using a rich set of interfaces and through the wide use of HTML and Java based Servlets.

Verisign - Provides a globally recognized certificate authority service along with a suite of products to support digital certificates. Using Verisign's OnSite service, the DMV could easily establish a certificate authority and being issue digital certificates. Verisign works primarily in web-based environments. Verisign provides server software components as well as a Personal Trust Agent that can be used for browser-based client-side key management functions. Enterprise functionality can be enhanced by the selection and use of third party tools from a number of partners.

RSA - RSA is one the leading cryptographic companies and is acquiring technology in this area to establish a full suite of product offerings. RSA BSAFE is a proven and mature cryptographic toolkit. With the acquisition of Xcert and Securant, RSA has added mature products to their offering and are integrating the products to create a full-featured suite of security solutions that include PKC.

Certicom - Certicom also provides a suite of products to support digital certificates and other cryptographic functions. Certicom provides a strong set of tools and products for wireless environments.

Chrysalis-ITS - Chrystalis-ITS provides HSM devices with varying degrees of security for cryptographic keying material including devices that comply with FIPS 140-1 Level 3 & 4 standards.

Rainbow Technologies - Rainbow provides a set of hardware cryptographic accelerators that can be used for a variety of purposes. Primarily, these devices are used in web-based environments to dramatically accelerate SSLv3 communications.

Ncipher - Similar to Rainbow, nCipher provides cryptographic accelerators that can be used for a variety of cryptographic purposes including certificate authorities and web servers.

IBM Cryptographic Coprocessors - IBM provides a range of cryptographic coprocessors and accelerators that are designed to run on a variety of IBM platforms including Intel based workstations, AIX, and OS/390 systems. Some coprocessors have been designed to comply with FIPS 140-1 Level 4, providing leading security for cryptographic keys.

Review Cycle

6 months

Access Control Sub-Component

Directory Services

Definition

An important component in an effective access control solution includes the use of enterprise directory services. These devices are similar to database servers, however, they are used by web servers or dedicated application servers, for determining a user's particular level of authorization, or access to, various information resources. These resources may range from a particular folder on a web server or URL, down to the granularity necessary at the file and database level. Directory servers do less than databases and are easier to manage and use. Applications can access the directory more easily using the directory API rather than using the standard SQL language used for general database access.

In addition to applications, network infrastructure will be the next eventual step in the use of directory services. With the growth of DEN, or Directory Enabled Networks, infrastructure is beginning to use directory services in managing user data traffic based upon the user attributes read from the directory server.

As the data is more static than a normal database, the server can be tuned to respond to hundreds of authentication requests per second. In addition to supporting LDAP, directory servers can support other protocols such as X.500 DAP, RADIUS (remote access protocol), HTTP (the Web access protocol), DNS (Internet name/address mapping protocol), and vendor proprietary protocols (e.g., Novell's NDS).

The following is a brief list of sample products that leverage directories:

1. Automated provisioning software
2. Customized web sites
3. User Management Systems
4. Network Management Systems
5. Virtual Private Networks
6. Sharable address books and Enterprise work management

Current and Future State

Current State	Future State
No current implementation of directory services for user information.	Development of a centralized directory containing user attributes. The directory will be used as the foundation for user authentication.
Limited implementations of directory services for use by applications. (Currently undergoing a pilot implementation of OpenLDAP)	Directory services will become a core component in future application architecture standards. In addition, the use of directories will be the key to providing authentication to DMV applications. The process is not an all-or-nothing scenario. Applications can be migrated selectively to allow for a controlled, smooth migration.

Guidelines

#	Directory Services Guidelines
1.	Support for directory services is required for all COTS and in-house development projects in use at the DMV **Rationale**: • With the growth of applications and services provided by the DMV, the use of DS is crucial in providing a manageable, centralized repository for user identification and authorization.
2.	Administration of access controls will be accomplished with the use of Provisioning standards and tools. **Rationale**: • Provisioning will work in conjunction with access controls for the automated creation and authorization of user accounts.

Standards

#	Directory Services Standards
1.	Directory services must be compliant with LDAP standards. **Rationale**: • LDAP has become the de-facto standard as the communication protocol for directory services. This protocol also supports SSL encryption, LDAPS, which may be a necessary security control feature for the DMV architecture.
2.	Directory products employed at the DMV will support chaining. **Rationale**: • Chaining refers to the ability to partition user data among multiple directory servers, while maintaining a single, logical view for the user.
3.	Directory products will support selective replication. **Rationale**: • Selective replication occurs when synchronizing multiple database servers which house a common directory. This feature is necessary for scalability and in providing redundancy for the directory.
4.	Attribute level security will be required for all directory products. **Rationale**: • Attributes are the individual entries within a specific user's account within a directory, e.g. their userid or group assignment, and are used for authentication and authorization. Therefore, attribute security is crucial feature of access control for directory services.
5.	Delegated administration will be required for all directory products. **Rationale**: • As the directory grows and requires partitioning among various servers, delegated administration will allow for distributive management for improved management capability.
6.	Directory products will support centralized management. **Rationale**: • Centralized management, along with delegated administration functionality, will allow for flexible and scalable management with an oversight capability.

#	Directory Services Standards
7.	Web-based administration will be required for all directory products. **Rationale**: • A web-enabled interface will be necessary for administrators and users to search, update, add, and delete information, including some self-service capabilities.
8.	Directory services must either have, or plan to support XML-based protocols for access, modifications, and basic directory functionality such as Directory Services Markup Language (DSML) **Rationale**: • XML-based protocols are the latest methods for accessing directory services and will work in conjunction with LDAP. Although still not ratified, definitions such as DSML are receiving wide acceptance in the industry and will provide a method for defining and accessing directory content.

Products

#	Directory Services Products
1.	**IBM OS/390 LDAP Server** Currently in place for the mainframe environment at TEALE. Was previously called IBM SecureWay.

Exceptions

The Department is currently implementing products that will be identified as exceptions to the current standards:

- DCE (Distributed Computing Environment)- this technology, based upon distributed directories is currently implemented at DMV headquarters and is used by DMV support staff, help desk, and DMVA developers for remote connectivity to field office devices.
- Open LDAP- used in the transfer of images to\from the Polaroid facility to Field Offices.

- Microsoft Active Directory – used in conjunction with the Microsoft Network Operating System supporting the DMV LAN.

Tech Watch

None

Review Cycle

6 months

Authentication

Definition

Authentication is the ability to assure that the person or machine that is connecting to a particular network, application, or service, is who they say they are. There are varying levels of authentication available:

1. **Minimal**-- No initial authentication is required to enter the application. Authentication is only performed upon a finalized purchase and is limited to address verification against the buyer's credit card number.
2. **Basic**--This is the familiar username and password process. This is sufficient to customize the user experience and set authorizations. Most applications still use this lower form of authentication. However, this basic approach is vulnerable to repudiation by one of the parties involved in the transaction, however, this must be balanced with the value of the items being traded and the cost of raising the assurance level.
3. **Digital Signatures**--This involves applying a digital certificate, Virtual Private Network (VPN), and/or smart cards on top of the username/password to raise the level of protection against repudiation. This in effect, creates an electronic signature for the user, and is a much stronger, legally enforceable electronic contract. This might be important for validation of extranet and remote users to a corporate network, used in the exchange of high-value goods, or where there are more than financial implications at stake, such as the submission of regulatory documents. This level of authentication is becoming the standard for eCommerce business. In addition, the task of authorization can be performed via the use of an LDAP server.
4. **Biometrics**--Raising the bar to indisputable authentication requires biometrics. This can only be justified when authentication is of the most critical importance. Biometrics is the use of physical characteristics for authentication; retinal scan, iris scan, facial, fingerprints, voice, etc. However, the increased cost and additional hardware requirements have resulted in a slower acceptance rate and small market share for the products at this time.

Current and Future State

Current State	Future State
Variety of authentication methods in place for users; Secure ID (PKI), host based, username\password, and limited use of digital certificates.	A centralized, core authentication and authorization architecture is to be developed based on existing and future development frameworks- CORBA, J2EE, Web Services, SODA.
RSA SecurID is used only for remote access users.	The RSA SecurID investment can be leverage to provide strong [two-factor] authentication for a variety of systems.

Guidelines

#	Authentication Guidelines
1.	All DMV employees (students, consultants, contractors, etc.) must meet a strong level of authentication for all electronic transactions performed. **Rationale**: • Employees' identification must be established when conducting business utilizing any DMV resources or on its behalf. This is used to establish an audit trail for tracking individual actions for security purposes- error detection, malicious activity, etc.
2.	Use of strong authentication tools will be required for verifying in-house and external user's credentials (i.e. password, user ID, personal identification number (PIN)). **Rationale**: • Dedicated authentication tools must be utilized for customers when conducting business with the DMV. The need for strong authentication is driven by the DMV's business need for non-repudiation when dealing with the public, as certain functions may have legal implications and its processes must support the legal standards for evidence.

Standards

#	Authentication Standards
1.	DMV will enforce password standards, e.g. length, expiration, syntax.
2.	Digital certificates will support the X.509 standard.
3.	Access control systems (ACS) will not exceed acceptable false accept rates.
4.	Access control systems will not exceed acceptable false reject rates.
5.	Access control systems will enable the portability and mobility of applications and users.
6.	ACS will employ two-factor authentication (e.g. something you have and something you know such as a token and PIN).
7.	The DMV will employ third-party credentials and clearinghouse networks.
8.	Certificate validations will be performed via Certificate Revocation Lists (CRLv2) and\or utilize the Online Certificate Status Protocol (OCSP).

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Authentication Products
1.	RSA SecurID Smart card technology currently in place at the DMV, used for authentication of remote users. Utilizes public key technology in the authentication of users via a time-based token.
2.	IBM Resource Access Control Facility (RACF) Currently in use at DMV. In addition to providing identification, authentication, and access control functionality for mainframe environments,

#	Authentication Products
	RACF also provides functionality for the logging and reporting of security-related events. RACF provides user interfaces for security administration and audit.

Tech Watch

- **Microsoft Passport & Liberty Alliance -** These two competing camps, organized by Microsoft and Sun, respectively, are currently developing a universal tool for allowing cross-platform and cross-application, cross-company, authentication and profile management for users. These two solutions are in their vision/formative stages and require significant product definitions, enhancements, and maturity over the near-term to be viable. Note, at this point, do not use either solution on systems requiring strong authentication, or those systems protecting sensitive information (these solutions have been known to introduce significant vulnerabilities).

- The use of digital certificates for authentication. Products to watch as potentially most suitable for use at the DMV include the products listed in the Cryptography and Key Management section and RSA Keon Advanced PKI, (which is a PKI implementation supporting digital certificates from any standards-based certificate authority (CA), user's private keys and credentials are protected in a single credential store, with security policy centrally managed by the system administrator. Can be used in conjunction with RSA SecurID smart cards or tokens, for two-factor authentication.)

- The use of biometrics for authentication. Biometrics is a very immature market, therefore attention should be paid to the emerging standards and its use; iris scan, retina, faceprint, fingerprint, etc. DMV should work closely with law enforcement agencies for the selection of the most appropriate biometric solution(s). At this early stage, products to watch as potentially most suitable for use at the DMV include Iridian Technologies Inc.– Panasonic Authenticam (Iris scanning tools provide the highest level of reliability among biometric devices. Non-intrusive, user scans performed 19 to 21 inches away, no physical contact. Allows workstation and enterprise logon for file, folder, and application level security. Immediate ROI due to elimination of need for password management costs.) and EyeDentify Inc.-Eyedentification (Retina scanning tool that can be coupled with smart card and networking technology for two-factor authentication.)

Review Cycle

6 months

Authorization

Definition

Once the individual has been identified, the user's authorization, or "rights" to an object must be determined. The tool used in determining authorization may take many forms, Access Control Lists (ACLs), LDAP directories, policy servers, etc.

Policy servers are security tools that handle the task of performing the authentication and authorization of users for both web-based and non-web applications or services. Some benefits that arise from the use of these tools include:

1. **Lowers network wide cost of ownership**. The complex task of managing the potentially millions of users in an e-business environment is automated and distributed throughout the organization. Manual tasks are eliminated, so implementing and managing the e-business can take less time and fewer resources. Business rules can be applied consistently throughout the e-business network because they are driven by one definitive, authoritative set of identity information.
2. **Shortens time to market**. Extensive XML and API capabilities accelerate the development of Internet applications.
3. **Strengthens security**. Changes to identity and policy information take effect immediately, eliminating the latency that creates vulnerability. Organizations can apply and manage different authentication methods, so each application gets the level of protection it needs.
4. **Increases user satisfaction and productivity**. E-Gov employees or partner agencies can sign on and receive access to all the application and resources they are entitled to. Their experience with the Department of Motor Vehicles will be more consistent, intuitive, and productive.
5. **DMV will not have to reengineer its network, applications, or processes**. Directory services can be smoothly integrated into the DMV's current application and e-business environment. It can be used with front-end portals, personalization solutions, and Web applications. Also, most policy server products reduce enterprise-wide costs by providing easy system-to-system integration through their extensive XML and API support.

Current and Future State

Current State	Future State
Variety of authorization methods in place for users; application-specific, security servers, web-servers.	Centralized, core authorization and authentication architecture to be developed.

Guidelines

#	Authorization Guidelines
1.	DMV will employ a centralized approach in its method of authorization **Rationale**: • Through the combined use of directory services, policy services, and portal software the Department of Motor Vehicles will centralize its user database and streamline the authorization process, for improved permissions management.

Standards

#	Authorization Standards
1.	Applications and e-Gov business tools will support the use of policy services **Rationale**: When employees and customers conduct business with the DMV, a centralized architecture will be in place for determining the permission levels to DMV resources and services.
2.	Authorization within applications will support high granularity- permissions at the resource level will be passed down to the data level. **Rationale**: Older authentication methods only required user permissions to be passed down to the application level. Authorization would then be performed to the data level by a single functional account with administrative rights. However, new tools have emerged which will allow individual permissions to be passed down to the data level, reducing the chance of account hijacking, and increasing the overall security of the database.
3.	The authorization products will support delegated administration **Rationale**: Delegated administration is a key feature for scalability of the solution. It provides the ability for the DMV to delegate administrative functions to appropriate personnel, and even

#	Authorization Standards
	directly to business partners.
4.	The authorization products will support dynamic rules **Rationale**: Dynamic rules are required to create scalable authorizations. Dynamic rules permit or deny access based on attributes contained within the users profile. If an attribute changes (i.e. preference, or status changes) then appropriate permissions can be enforced based on the change without necessitating a manual update to the access control list (or group membership).
5.	The authorization products will support the Security Assertion Markup Language (SAML) **Rationale**: SAML is becoming a widely accepted XML-based standard for security assertions across enterprises and is supported by many security product vendors, including authentication, authorization, and attribute assertions.

Products

#	Authorization Products
1.	One Point- Directory and Resource Administrator **Rationale**: Product currently purchased, but not yet implemented within DMV.
2.	**IBM Tivoli Access Manger** **Rationale**: Provides a solution for securing web-based applications and can simplify application coding. Supports a variety of authentication techniques such as digital certificates and tokens without requiring any change on supported applications. Was previously called Tivoli Secureway Policy Director.

Tech Watch

Authorization products (e.g. policy services) are still relatively immature, therefore current products should be re-evaluated. The security products listed below such as Oblix, Netegrity, and RSA/Security provide authentication and access control solutions that are suited to certain web-based environments. These products do not provide application-level, contextual, authorization and therefore do not replace the functionality available in the DMV's enterprise applications. Care needs to be exercised in the

implementation and deployment of these tools to maximize the benefit (and justify the cost). The DMV should take steps to minimize the disparate application technologies and consider security middleware tools such before contemplating the authentication and access control products. Quadrasis EASI, and other middleware products like it, provide a framework for integrating security across the distributed enterprise and can be used to integrate the security point solutions.

The technologies and products to watch as potentially most suitable for use at the DMV are listed below:

LDAP is the current de-facto standard for policy services\ directory functionality, however, DSML is gaining and looks to be the eventually replacement. Microsoft also has its own protocol, Active Directory Service Interface (ADSI), which may eventually gain some market share, but is compatible with other protocols; LDAP, NDS, etc.

- **Quadrasis Enterprise Application Security Integration (EASI) -** Provides a security "middleware" tool for integrating security into EJB and CORBA environments. Provides a solution for implementing security (including authentication and authorization) across the distributed enterprise and integrating a broad set of enterprise technologies. Provides a critical layer of abstraction for integrating a variety of security point solutions and eliminating dependence on particular vendors. EASI helps to ensure uniformity across the enterprise and relies on messaging technologies such as SAML to deliver its capabilities. It can be used to create a uniform security solution for the DMV's applications and position the DMV to benefit from the security point solutions as the market matures.

- **Oblix NetPoint** – Offers delegated policy and identity administration, superior Identity Management (creation, deletion, and modification of user, group, and organization identity information for the entire enterprise), single sign-on for resources across multiple DNS domains, integrated management with Verisign for certificate authentication.

- **Netegrity Siteminder** - High scalability; delegated administration, user self-registration of profile information into a directory, Netegrity Affiliate Services- allows passing of user credentials and entitlement information to affiliate and partner sites, broad support of authentication methods- passwords, token cards, X.509 public-key certificates, custom forms, biometrics, or a combination of methods.

- **RSA/Securant ClearTrust** - Plug-and-play integration with existing directory services, authentication services, PKI, Web servers and application servers; Smart Rules- for building authorization and user privilege policies based on static and dynamic user profile data, and allows efficient mapping of business rules to authorization policies, and performs end to end auditing of all transactions, providing for non-repudiation of transactions by partners, suppliers, and customers.

- **Novell iChain** - Policy-based management software that controls access to application, web, and network resources. Supports several types of authentication methods, including smart card, username/password, and token authentication (RADIUS). User completes a self-service form, stored on the directory server and used for authentication, providing reduced sign-on for connecting to other web-based applications. Integrates with a proxy server for eliminating redundant user requests to the Web server.

Review Cycle

6 months

Remote Access

Definition

Remote access is a compulsory function required in the DMV environment to provide user access to resources from remote locations. These locations may include: an employee working from home, hotels, airports, etc. Users will access a variety of systems and the security of those systems becomes essential when remote access is implemented. Remote access solutions vary significantly and if not deployed securely can introduce significant vulnerabilities into the enterprise. Indeed, remote access is a common method used by intruders to gain access to systems.

Remote access solutions that can be considered by the DMV include direct dial, leased line, Integrated Services Digital Network (ISDN), DSL (Digital Subscriber Line), Virtual Private Network, wireless, and via the Internet. Furthermore, there are choices with the underlying protocols that can be employed by the various remote access solutions including PPTP, IPSec, and SSH. Additionally, the DMV can “webify” applications and provide remote access through the web, using SSL for authentication and encryption.

The technology, interoperability, effort, costs, operations, and security associated with the options differ significantly. The potential need for the DMV to support several remote access options and technologies, depending on business requirements, can complicate the security measures.

The objective for DMV is to implement a remote access solution that maintains consistency with the overall security architecture and to leverage the security mechanisms built into the environment. In addition, the objective is to ensure that remote access is uniform and simplified for all users. The uniformity will bring an added degree of security and simplified administration. The potential for cost reduction is another consideration when looking at remote access solutions, as well as reducing the points of entry for an intruder into the network. Limiting the points of entry can enhance the capabilities of other security solutions such as Intrusion Detection Systems.

This Sub-Component will address the security needs for the DMV to offer remote access to users. The scope of this effort will not address the security requirements of wide area networks such as network-to-network communications between office locations.

Current and Future State

Current State	Future State
Disparate authentication utilized	Standardized and consistent authentication methods should be deployed.
Multiple points of entry are introduced into the environment.	Ensure that all traffic is funneled through a single choke point.

Guidelines

#	Remote Access Guidelines
1.	The preferred method for remote access will be through web-based interfaces and will leverage a variety of web technologies (XML, XSLT, XHTML, HTML, CSS) to reach the maximum number of web-based devices **Rationale**: • The DMV will strive to "webify" back-end applications and processes in order to provide remote access to users. This will leverage standards based communications (HTTP) and a ubiquitous interface (browser) for remote access from a myriad of locations, including home computers, business partner computers, kiosks, and PDAs, and a variety of web enabled applications on different operating systems (Windows, Mac, Linux, Solaris, and hardware appliances). The DMV will also be able to leverage web-based security tools such as SSLv3 mutual authentication, and web server authorization[1].
2.	Establish uniform remote access to all systems **Rationale**: • Uniform access will simplify the technologies and operations that are required to support remote access. The uniformity will also simplify the security requirements and provide an added degree of security by reducing errors and omissions that would be inherent in complex infrastructures.
3.	Utilize standardized authentication for remote access

[1] The single sign-on and access control products listed in the Authentication and Authorization Sub-Components can be used for remote access security if the DMV "webifies" the interface.

#	Remote Access Guidelines
	Rationale: • Utilizing a standardized authentication scheme will leverage security measures inherent throughout the DMV environment and permit the remote access solution to remain in compliance with DMV policies. Ensuring that the remote access solution utilizes a standardized authentication mechanism will also support the need to provide users with "reduced login". Additional security can be realized by eliminating the need for users to remember yet another ID and password, or to carry a token that is unique to the remote access solution.
4.	No modems to be installed on workstations connected to the Department's LAN **Rationale**: • Use of a modem on a DMV workstation circumvents all security controls currently in place for external access to DMV resources.

Standards

#	Remote Access Standards
1.	Encryption protocols to be implemented for all remote access sessions **Rationale**: • Remote access communications are inherently insecure as they generally pass through public networks and the point of entry into the network is generally not known ahead of time. Although point-to-point communications can offer more security than shared network communications, it is preferred to have a consistent and standard scheme for communications. For this reason, encrypted communications utilizing PPTP, IPSec/IKE, SSH, etc. is required for all remote access communications.
2.	DMV staff working from remote locations will have desktop firewall software, and/or personal firewall appliances installed **Rationale**: • Desktop firewall products protect data located on DMV resources that are sensitive to external attacks or probes- i.e. port scans. Telecommuters which have "always on" connections, such as Digital Subscriber Lines (DSL) or cable modems are most susceptible.

Products

#	Remote Access Products
	No products are currently approved for use at the DMV within this Sub-Component.

Tech Watch

- Remote access products to watch as potentially most suitable for use at the DMV include AT&T Remote Access Services (Allows customer to access a global network and authorized services using remote dial from various types of data communication equipment; LANs, workstations with terminal emulators, ISDN, etc.) and WorldCom Remote Access (Allows customer to access a global network and authorized services using remote dial from various types of data communication equipment; LANs, workstations with terminal emulators, ISDN, etc.)

- VPN products to watch as potentially most suitable for use at the DMV include AT&T IP Remote Access, Internet VPN Gateway (Permits users to access their company's internal resources by leveraging the global AT&T network), WorldCom Total Access IP VPN (Permits users to access their company's internal resources by leveraging the WorldCom global network) and Checkpoint VPN (Market leading VPN solution, provides encrypted communications over public networks. Provides easy integration with its FW-1 perimeter firewall product)

Review Cycle

1 year

Computer Security Operations Sub-Component

Auditing Tools

Definition

Auditing tools record a series of computer events, about an operating system, an application, or user activities. A computer system may have several audit trails, each devoted to a particular type of activity. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

A system can maintain several different audit trails concurrently. There are typically two kinds of audit records, (1) an event-oriented log and (2) a record of every keystroke, often called keystroke monitoring. Event-based logs usually contain records describing system events, application events, or user events.

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result. Date and time can help determine if the user was a masquerader or the actual person specified. Auditing tools can help organize the audit log files so that the results are prioritized and present useful information.

Current and Future State

Current State	Future State
Security logs reviewed by various disparate groups; Network Infrastructure Support (ISD), server admins, TEALE, etc. Due to resource limitations, logs are not always reviewed as often as necessary.	Development of a dedicated and centralized security operations team that is security certified and sufficiently staffed to review logs as defined by DMV security policies.

Guidelines

#	Auditing Tools Guidelines
1.	Protect system logs and audit trail data with the minimum set of controls required by the most sensitive/classified type of system being tracked. **Rationale**: • This information must be protected to keep the integrity of the data for analysis, and also to ensure the confidentiality of the data.
2.	Audit logs must be reviewed periodically to be effective **Rationale**: • Audit logs have no value if they are not viewed on a regular basis. If left unattended, the size of the logs can become overwhelming making analysis more difficult.
3.	To the extent possible, system logs and audit trails should be centralized for tracking, monitoring, archiving, and analysis **Rationale**: • Centralized logging facilities provide an additional level of security for the proper handling of event tracking, including the archiving of data and forensic analysis. Central logging facilities including servers, software components, and hardware can provide standardized control over audit trails and system logs, as well as ensures compliance with applicable records retention laws such as the Federal Electronic Signature Act. Centralized logging facilities are not possible in all cases, in this event, the DMV should take steps to minimize independent logging and create standards for specific platforms (e.g. mainframe, Windows, and Unix).
4.	Develop standards for system wide logging including configuration of log events, log structures, log entry fields, and log processing **Rationale**: • A set of standards must be followed by all applications to ensure consistency, completeness, ease of administration & support, and integrity of the system-wide logging and audit trail process. The established standards must address the need for log formats including the need for date/time stamps, user identification, event type, event detail, and success/failure notification. Log configuration is an essential function and is required to increase and decrease the amount of logging that a system performs—to address the operational requirements at the time. In addition, standards are to be developed for log processing including the collection and analysis of log data.

#	Auditing Tools Guidelines
5.	The DMV will enforce separation of duty policies for the handling of audit trails **Rationale**: • Audit trails are a critical element in the balance and control measures that the DMV will rely on for security. The integrity of Audit Trails must be maintained to provide assurances to auditors, forensic investigators, and troubleshooters. Separation of duties is essential for integrity.

Standards

#	Auditing Tools Standards
1.	Syslog will be utilized by applications and systems which support it, for providing centralized logging **Rationale**: • Due to the wide support for syslog, the DMV will leverage this tool to provide for management and centralized control over its system logs.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Auditing Tools Products
1.	Syslog Although stemming from the Unix environment, syslog provides a standard set of protocols and logging structures supported by a variety of environments and applications including operating systems, network devices, third party applications, and Java. There are even utilities to integrate Microsoft's Event Log with syslog. Many third party applications (freeware, shareware, and commercial) are available to support centralized syslog functionality as well as analysis of the event logs.

#	Auditing Tools Products
2.	Microsoft Windows Event Log Microsoft provides event-logging capabilities for Windows environments and includes functionality to view events and administer log files. The logging facility is supported by a wide variety of Windows based applications. Third party tools are available to integrate Windows event logs with syslog.
3.	IBM Resource Access Control Facility (RACF) Currently in use at DMV. In addition to providing identification, authentication, and access control functionality for mainframe environments, RACF also provides functionality for the logging and reporting of security-related events. RACF provides user interfaces for security administration and audit.
4.	Microsoft Site Server Currently in use at DMV for intranet web servers. Allows for publishing, retrieval, and information sharing. Extensive searching capability, including tools for performing analyses of the site's usage and effectiveness.

Tech Watch

Products to watch as potentially most suitable for use at the DMV are listed below:

- **Network Flight Recorder's Secure Log Repository (SLR)** - Aggregates log entries from multiple sources for analysis and reporting. SLR also supports filtering and notifications of specific events. SLR ensures that log data is protected against tampering or accidental erasure. In addition, SLR's solution (server and agents) provides secure communication of log file entries. SLR supports Syslog.

- **ISS Secure Log Manager -** Provides a facility to centralize log entries from individual systems, and allows for centralized administration. Log entries are securely transferred. Additional features include viewing log entries, archiving, and export to an ODBC database.

- **WebTrends -** Provides a suite of trend analysis tools for web-based traffic. They also offer log file analysis and firewall reporting products. As with the system hardening, and vulnerability scanning products, these will be useful tools (as part of a toolkit) for analyzing log files generated by a variety of systems.

Review Cycle

1 year

Desktop Protection

Definition

Information is most accessible from user desktop workstations. It is necessary to secure these systems in a manner that unintended use of the systems is reduced. Not only is information accessible on these systems, but also as they are also attached to other servers and devices through the network, the risks are multiplied. Desktop protection refers to the proper and safe usage of these systems so that internal threats can be limited.

Current and Future State

Current State	Future State
Password time out restrictions in place for idle desktop systems	Maintain current environment
Remote users do not currently employ physical controls for systems	Distribute physical controls for remote users in deterring theft, such as cable locks, asset tags, etc.

Guidelines

#	Desktop Protection Guidelines
1.	Provide physical deterrents to theft for computing assets **Rationale**: • Computing assets such as workstations and laptops are vulnerable to theft and in all likelihood will contain a wealth of information. Physical deterrents are to be used to prevent theft. The deterrent used will vary depending on the type and value of the computing asset and where it will be deployed. Deterrents can include secure facilities, cables & locks, asset tags, electronic tags, and other reasonable means.
2.	Provide logical deterrents to information theft, such as encryption, for laptops in insecure environments **Rationale**: • Laptops are vulnerable to theft and can contain a wealth of information; therefore laptops must provide a facility to logically protect information even in the event of its theft. Encryption techniques can be employed to provide logical protection.

#	Desktop Protection Guidelines
3.	Users will not be allowed to load any unauthorized software on DMV workstations or laptops **Rationale**: • In addition to causing conflicts with the workstation or laptop's functionality, users loading untested and unapproved software run the risk of installing malicious code e.g. viruses, trojan horses, etc.

Standards

#	Desktop Protection Standards
1.	Password authentication required to access any desktop system **Rationale**: • Making authentication a requirement to use a desktop makes the information only accessible to valid users.
2.	Implement time-out password requirements for idle desktop systems **Rationale**: • If a system is left unattended, it is vulnerable to any person passing by that system. The time-out period should be relatively short so that the system is not left unattended and unprotected for an extended period of time
4.	Operating system controls to be used for restricting user installation of unauthorized software\hardware. **Rationale**: • By limiting the user's administrative rights on the machine, the Department can eliminate the risk of a user unintentionally compromising the security of their system through unauthorized installations.
5.	Laptop computers will use secure asset tags.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Desktop Protection Products
1.	STOP Asset Tags Unique, tamper-proof patented plates, which are placed on laptops, etc. Uses a barcode and indelible tattoo to mark and prevent the theft and resale of equipment. Plates are linked to an international tracking database accessible via a 7x24 telephone support line. Barcode on tag allows for easy tracking and inventory.
2.	RSA Keon Desktop Used with RSA Keon Security Server, implements PKI technology through the desktop's virtual smart card Credential Store to securely downloaded certificates to the user anywhere on the network, allowing them access to their digital credentials and lock or terminate their desktop session at any time. Desktop sessions can also be locked or terminated if an optional smart card is removed from the reader.

Tech Watch

- Monitor Windows 2000 and the inherent OS security within the product- NTFS, EFS (Encrypted File System) which allows user to control access to local or network resources.

Review Cycle

1 year

Messaging Security

Definition

Messaging is an essential ingredient in every technology environment and is responsible for communication between applications and people. Messaging systems take many forms and include the most ubiquitous form of messaging: electronic mail. Messaging has taken center stage of late with the advent of the Extensible Markup Language (XML) and the myriad of XML messaging protocols that have evolved to address business-to-business and application-to-application requirements. Although, enterprise-messaging solutions have been around for several years including the many forms of Enterprise Application Integration, the burgeoning XML messaging market has created tremendous interest in this area, as well as introduced a significant number of variables for security.

The XML messaging efforts that are underway to enable business-to-business communications have highlighted the need for message-based security. This need is to address the requirements for integrity, confidentiality, availability, and accountability in message based transactions. Security solutions must have the ability to provide functionality in the areas of authentication, entitlements, and routing. These measures must also account for the distributed, un-tethered nature of autonomous messages.

The security solutions sought and implemented by the DMV will be broad and diverse in order to provide an effective capability for the different messaging infrastructures used in the DMV environment. The goal with the architecture is to provide a solid foundation that can build upon standard security techniques, processes, and technologies. Areas for architecture focus include:

1. The use of public key infrastructure and cryptography to provide integrity and confidentiality.
2. The use of emerging XML-based standards such as SAML and XMLDSIG.
3. The use of Web Services to provide a supporting infrastructure for security in Internet, Extranet, and Enterprise Integration environments.
4. The use of application security framework tools to provide the functionality required to support message-based security.
5. The use of commercial software to integrate with user-based applications such as electronic mail.

Electronic mail is still a pervasive method for communication both inside and outside the enterprise. It is used both for personal communication and for application-to-application messaging such as that used for EDI over the Internet. With electronic mail, many different organizations will handle a message as it travels to the destination; and

all will have the capability to read the message unless appropriate measures are taken. Standard electronic mail is neither encrypted nor authenticated and has similar security to that of a postcard. Security for electronic mail is not widely accepted and different methods exist for assuring confidentiality and integrity. One method is S/MIME, which is security over a current standard of email messages called MIME. Though S/MIME encrypts the contents of a message, the sender and recipient information is not and can present a risk in some environments. Another form of encryption is Pretty Good Privacy (PGP), which uses public key encryption to encrypt the message and verify the sender using digital signatures. However, neither of these methods has yet emerged to become a widely accepted (de-facto) standard.

Messaging security addresses means to secure information as it travels across different systems both inside and outside the organization, as well as using many different transport mechanisms. Messaging security requires many of the subcomponents in security such as cryptography, authentication and certification tools.

Current and Future State

Current State	Future State
DMV email policy listed within the security documentation. No assurance that users are aware of the policy. All current and new employees to sign HR document which states they are aware of the DMV policy regarding proper use of email.	No current implementation of email encryption. Utilize email software that will allow employees to manually encrypt sensitive messages crossing public networks.
No standard security controls are implemented for messaging infrastructure	A standard set of security controls will be implemented for all messaging infrastructures including MQSeries, XML, and electronic mail.

Guidelines

#	Messaging Security Guidelines
1.	Sensitive information leaving the organization shall be encrypted to ensure data integrity. **Rationale**: • Information on the Internet spans many different networks and many different organizations. If this information is not encrypted, then its confidentiality and integrity may be compromised.
2.	Electronic mail is to be handled and managed similar to first-class mail in the traditional postal environment. **Rationale**: • Rather than being treated similar to a postcard, electronic mail will receive the same treatment and first-class mail with respect to confidentiality.
3.	Electronic mail use will be in accordance with the DMV's acceptable use policies. **Rationale:** • The use of email is a tool provided by the organization to facilitate productivity for the company and is to be used primarily for business related activities. In addition to costs associated with lost productivity from non-business use, risks arise due to emails that can contain viruses or other malicious code.
4.	Internal messaging infrastructures will implement authentication and access control security measures to protect access to vital messaging components such as queues. **Rationale**: • Messaging infrastructures (i.e. "middleware") are used to communicate sensitive transactions and information between enterprise systems. Access to the messaging infrastructure must be controlled to protect the integrity of systems communicating over the messaging-bus.
5.	Session encryption will be used by the messaging infrastructure to protect sensitive communications **Rationale**: • Sensitive information that is communicated across networks must be encrypted to protect the confidentiality.

#	Messaging Security Guidelines
6.	Where feasible, a single standardized messaging infrastructure should be implemented within the DMV **Rationale**: • Standardizing on a single messaging infrastructure will lower operating costs, ease integration requirements, and improve the deployment of security controls.
7.	The messaging infrastructure must support the passing of user credentials **Rationale**: • Although messaging infrastructures may not authenticate end-users, they will need to pass these user credentials to applications for identification and possibly application-level authentication and authorization.

Standards

#	Messaging Security Standards
1.	The use of S/MIME for the secure transfer of electronic messages. **Rationale**: • S/MIME provides a standard format for securing the contents of messages.
2.	The use of X.509 digital certificates for identification and authentication. **Rationale**: • X.509 is the accepted standard for digital certificates and is a widely accepted method for digital authentication. X.509 can be used in un-tethered environments as well as environments that require 3rd party identity validation and authentication.
3.	The use of Security Assertion Markup Language (SAML) for inter-enterprise authentication and authorization. **Rationale**: • SAML is becoming a widely accepted XML-based standard for security assertions across enterprises and is supported by many security product vendors.

#	Messaging Security Standards
4.	The DMV will implement SSLv3 (or TLS 1.0) as the primary security protocol for protecting web-based communications **Rationale**: • SSLv3 (TLS 1.0) has become the tried-and-tested defacto standard for protecting HTTP communications (i.e. HTTPS). SSLv3 supports a variety of encryption schemes and the DMV will support at least 128-bit encryption. SSLv3 also supports client and server side (mutual) authentication that is important for message-based communications. e-Business communications, such as SOAP, will likely take place using HTTP as the transport protocol. SSLv3 is the accepted security protocol and is support by numerous third party applications including web servers and application servers. SSLv3 security is also available for MQSeries.

Products

#	Messaging Security Products
1.	MQSeries SupportPac SupportPac provides security services at the middleware level. That is, it integrates with the MQSeries channels as channel exit programs that are based on the GSS-API specification (a well defined, open security API standard). When used with products such as Entrust's Session toolkit (which supports GSS-API), SupportPac will provide Queue Manager Authentication, Message Integrity, and Message Privacy.

Tech Watch

- **Monitor the XMLDSIG** - this is a work in progress and is being driven out of the W3C efforts. XMLDSIG specifies digital signature processing rules and syntax. XML digital signatures provide integrity, message authentication, and/or signer authentication services for data of any type. XMLDSIG can be included as a digest within another XML message.

- **Monitor the XMLENC** - This is a work in progress being driven out of the W3C efforts. XMLENC provides a process for encrypting data and representing that result in XML. The data maybe arbitrary, an XML element, or XML element content. The result of the encryption process is an XML Encryption element, which contains or references the cipher (encrypted) data.

- **XACL -** This is a work in progress through the W3C and is proposed by IBM. XACL provides a process and syntax for specifying XML access controls that can be applied to messages.

- **Monitor SOAP Security Extensions**, which will be determined in future SOAP specifications.

- **Monitor the XKMS -** The XML Key Management System was defined and proposed as a standard for extending PKI into the realm of XML. The intent is to improve PKI interoperability by using XML. Several toolkits are available that support XKMS, including Verisign and Entrust. XKMS is also being integrated in Microsoft's .Net Framework. XKMS can be used to provide trust services over the Internet and permit secure message exchanges between business partners.

- **W3C and competing standards efforts** - The XML messaging solutions are being heavily debated and several competing solutions are proposed to the W3C. Watch this market closely.

- **Security Middleware -** The use of security "middleware" tools for messaging can help the Department position itself to tap the market as it matures. A market-leading product to monitor is Quadrasis Enterprise Application Security Integration (EASI) – (Quadrasis provides a security "middleware" tool for integrating security into EJB and CORBA environments. Quadrasis provides a solution for implementing security across the distributed enterprise and integrating a broad set of enterprise technologies. Quadrasis provides a critical layer of abstraction for integrating a variety of security point solutions and eliminating dependence on particular vendors. EASI is a necessary component to ensure uniformity across the enterprise and relies on messaging technologies such as SAML to deliver its capabilities. Quadrasis can be used to create a uniform security solution for the DMV's messaging infrastructure.)

Products to watch as potentially most suitable for use at the DMV are listed below:

- **Public Key Infrastructure products (see Cryptography and Key Management section)** - The digital certificate capabilities of the products highlighted in the Cryptography and Key Management section can be used to leverage the SSLv3 and S/MIME functionality inherent in a variety of applications including electronic mail, web servers, and application servers This solution will leverage capabilities inherent in existing DMV applications and integrating digital certificates (see Cryptography and Key Management for additional details).

- **Microsoft .Net -** Microsoft has built messaging security capabilities into the .Net framework and also relies on SSLv3 encryption and authentication for HTTP based traffic. Microsoft has also partnered with Verisign to add PKI security into Passport.

- **IBM XML Security Suite -** The XML Security Suite is a tool that provides message-level security features such as digital signatures, encryption, and access control for XML documents. This type of functionality goes beyond the typical session based security provided by SSLv3 and provides true end-to-end security capabilities.

- **Tivoli Secureway Policy Director for MQSeries -** Policy Director for MQSeries is a comprehensive security suite for IBM's MQSeries, and enables applications to securely communicate across a variety of platforms. Policy Director allows systems to verify integrity and protect confidentiality.

Review Cycle

6 months.

Anti-virus

Definition

Virus-checking products are the best defense against viruses. The products scan all incoming files and run on individual systems or on a perimeter device such as a firewall. Virus-checking software scans the contents of a file, looking for patterns or signatures that are known to be part of a virus. Virus-checking software requires a configuration file or database containing the virus signatures for which it is scanning. Thus only viruses known by the authors of the virus-checking products can be found, and the configuration file containing virus signatures needs to be continually updated as new viruses are found. All virus vendors offer on-line mechanisms for updating their signature files. Hence, the more frequent the updates, the better the level of protection.

Current and Future State

Current State	Future State
Anti-virus systems in place for firewall, email, web, and user systems	Maintain current environment.

Guidelines

#	Anti-Virus Guidelines
1.	Only systems personnel can load system software **Rationale**: • If administrative controls over software are not enforced, the system is more vulnerable to viruses, to unexpected software interactions, and to software that may subvert or bypass security controls.
2.	Anti-virus programs are to be loaded onto network resources identified as being vulnerable to virus attacks **Rationale**: • To prevent external attacks, this is a crucial feature for all nodes which communicate over the Internet- HTTP, Firewall, SMTP, user systems, etc.

#	Anti-Virus Guidelines
3.	Users will not be allowed to load any unauthorized software on DMV workstations or laptops **Rationale:** • In addition to causing conflicts with the workstation or laptop's functionality, users loading untested and unapproved software run the risk of installing malicious code e.g. viruses, trojan horses, etc.
4.	The DMV will frequently update anti-virus definition files and virus recognition patterns **Rationale**: • The definition files must be up to date to ensure that the anti-virus software recognizes the latest threats.

Standards

#	Anti-Virus Standards
	None

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Anti-Virus Products
1.	Norton Anti-Virus Corporate Edition Enforceable anti-virus policy management provided across multiple platforms. Single management console. Industry leading technology. Currently in use at the workstation level within DMV.
2.	McAfee GroupShield Exchange Remote management capability- fully integrated with MMC (Microsoft Management Console).

#	Anti-Virus Products
	Excellent content filtering- files can be blocked or quarantined by subject line, file attachment name, file type and file size. Proactive “Outbreak Manager” looks for suspicious 'outbreak' like e-mail behavioral patterns. Currently in use at the file server level within DMV.
3.	Aladdin eSafe Gateway Manages email traffic based on corporate policies for blocking and scanning: dangerous attachments, malicious scripts, spam, spoofed mail, and other hostile content. Scalable, high-availability architecture. Currently in use at the firewall level within DMV.
4.	Trend Micro Server Protect Anti-virus product currently in use on file server systems at DMV. Safeguards multiple servers and domains from virus attack with next-generation software. Real-time scanning capability; uses both rule-based and pattern-recognition technology to detect and remove both known and unknown viruses, including all "in-the-wild" viruses. Detects the activity of Trojan horse programs and recovers system files that have been modified.

Tech Watch

- No new technology on the horizon, as this is a mature product market.

Review Cycle

None

Telecommunications & Network Security Sub-Component

Intrusion Detection Systems

Definition

Intrusions are a foregone conclusion in any environment. The ability of an organization to recognize and respond to an intrusion is critical for assuring the security of the systems. Intrusion Detection Systems (IDS) provide the technical ability to detect intrusions, and established processes and training provide the ability analyze results and respond quickly and correctly. A variety of IDS solutions are available on the market with each product utilizing different methods and heuristics for detecting and properly identifying intrusions. In addition, proper awareness training of operations staff can provide an additional (human) level of detection to possible intrusions.

IDS technologies fall into several categories including Network, Host, and Application. Network based IDS products employ monitors to watch network traffic for intrusion "signatures". Host based solutions provide agents that are installed on servers to monitor system logs for potential intrusions. Application based IDS products work directly with applications (such as those that are web-based) to monitor application transactions for potential intrusions. The success or failure of these solutions depends directly on their deployment, configuration, and operations.

The goal for the DMV will be to deploy an effective network of IDS capabilities to monitor key points in the environment, as it is impractical and inefficient to monitor the entire environment. As a precursor to the IDS deployment the DMV will perform a risk assessment to identify prospective exposures and threats and use the results to guide the deployment of the IDS network. The DMV will ensure that this network is positioned, configured, and monitored effectively to detect potential intrusions. In conjunction with this effort, proper training is required for internal staff to recognize actual intrusions and to reduce false-positives.

Current and Future State

Current State	Future State
IDS systems are deployed based on results from a technical evaluation, not a formal risk assessment	Risk assessment results are used to determine the proper deployment and configuration of IDS tools
Network and Host based intrusion detection tools are currently in use	Continue with the use of IDS, with the assurance that the correct deployment and configuration of the tools are being implemented

Guidelines

#	Intrusion Detection Guidelines
1.	Risk assessments will be conducted to identify exposures and threats. **Rationale**: • Risk assessments are critical tools for identifying exposures and threats to the DMV systems with some precision. The assessments will also identify key information assets (such as trade secrets) that warrant extra security measures. The results from the assessment are required to effectively deploy and configure IDS solutions.
2.	An effective network of IDS capabilities will be deployed based on the identified risks. **Rationale**: • An IDS network will be deployed and configured to monitor high-risk elements of the DMV environment. This network must utilize the appropriate IDS methods and heuristics to properly identify “true” intrusions.
3.	Intrusion response procedures will be developed and will be coordinated with TEALE. **Rationale**: • IDS solutions are ineffectual unless response procedures are developed to analyze results, and respond appropriately and correctly.

#	Intrusion Detection Guidelines
4.	Centralized DMV unit will be properly trained to operate IDS technologies and respond to intrusions. **Rationale**: • Specific DMV staff will need to be trained on the implementation, maintenance, and operation of IDS technologies. In addition, these staff members will require formal training on the response procedures and guidelines.
5.	The security awareness program will be enhanced to include topics on identifying and responding to potential intrusions. **Rationale**: • DMV IT staff provide extra "eyes-and-ears" for detecting intrusions. Proper training will assist in educating DMV IT staff in recognizing potential intrusions and appropriately responding. The program also heightens the awareness among DMV IT staff.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Intrusion Detection Products
1.	SNORT A freeware IDS that is currently in use at the DMV. A packet sniffer and logger that can be used as a lightweight network intrusion detection system (NIDS). It features rules based logging to perform content pattern matching and detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, etc. Offers real-time alerting capability, with alerts being sent to syslog, Server Message Block (SMB) "WinPopup" messages, or a separate "alert" file.
2.	Cisco Secure IDS High-speed network security "appliance" that analyzes traffic and detects unauthorized activity traversing the network and attacks by hackers. Sends alarms to a management console with details of the activity. IDS can be integrated with other Cisco infrastructure- firewalls, routers, and switches, via Cisco Sensor appliances. Dynamic infrastructure responses to threats- e.g. can monitor and change a router's access control list (ACL). Currently in use at DMV.

#	Intrusion Detection Products
3.	Cisco IDS Host Sensor Proactively protects application and web hosts by evaluating requests to the operating system and the application-programming interface (API) before they are processed. Integration with management systems. Complements the DMV's existing security infrastructure. Security events can generate a variety of notifications, eliminating the need for constant monitoring of console.
4.	ISS RealSecure Network Sensor Market leading technology. Runs on dedicated workstations to provide unmatched network intrusion detection and response. Can terminate the connection, send email or pager alerts, record the session, reconfigure select firewalls, send alarms to third-party management consoles or take other, user-directed actions.
5.	ISS RealSecure OS Sensor Host-based complement to RealSecure Network Sensor. Analyzes host logs to identify attacks, determine whether the attack was successful, and provide valuable forensic information. Can terminate user processes and\or suspend user accounts when suspicious activity is detected.

Tech Watch

No current technology on the horizon, as this is a mature product market.

Review Cycle

1 year

Configuration Management

**This section has been addressed in the Systems Management Component. Please refer to this Component for standards and products.

Application & Systems Development Sub-Component

Application Authentication and Single Sign-on (SSO)

Definition

Single Sign-On (SSO) refers to the concept of allowing a user one ID and password combination for access across multiple systems to all necessary applications or services. SSO is a process that involves authenticating the user and then authorizing the user to access multiple resources. These resources can be application specific or for web resources, such as access to a particular URL or folder on a web server.

The user ID and password is stored in a specialized database called a directory, and is usually accessed via LDAP to handle the authentication. Directories also hold and provide access to "attributes," or permissions, which are used by applications or policy servers that perform the authorization for them. Authorization services are carried out by a policy management application that can determine if a user can or cannot access a resource. This information should be centrally located as well as redundant, to support high availability. Unfortunately, the technology for these products is relatively immature at this time and its functionality in creating "true" single sign-on is limited. However, the tools are successful in reducing the number of accounts for which a user is responsible.

Current and Future State

Current State	Future State
Authentication methods vary and are application-specific. Mixed reactions from groups within DMV as to the necessity of a SSO solution.	Continue discussion and research into the necessity of SSO for DMV.

Guidelines

#	Application Authentication and Single Sign-On (SSO) Guidelines
1.	Application authentication and SSO must provide options for strong authentication (i.e. biometrics, two-factor authentication) **Rationale**: • Authentication schemes and the use of strong passwords make access to the systems more secure.
2.	Centralized administration **Rationale**: • Administration of a user's authorization must be centralized so that access can be granted in one location, thereby improving user account management and application security.
3.	Original user or resource credentials must be passed by the application to other connected systems, for providing granular level permissions **Rationale**: • Passing credentials of the user or resource that originally authenticates is critical for ensuring that the proper authorization rules are applied. This is in contrast to a user or resource authenticating to a front-end application (such as a web server), and that application authenticating itself to a back-end system—where only the applications rights and privileges are enforced, rather than the users. In practice, this creates an exposure since the application will in all likelihood have greater privileges than the user—presenting an opportunity for the user to possibly gain unauthorized access to information.
4.	The DMV will make all possible attempts to create a common ID across all applications • **Rationale**: A common ID will simplify user tracking and identification. It will also eliminate the need for the user to remember multiple ID's.

Standards

#	Application Authentication and Single Sign-On (SSO) Standards
1.	Use industry standard protocols for authentication and data retrieval

#	Application Authentication and Single Sign-On (SSO) Standards
	Rationale: • With large environments, searches utilizing LDAP is more efficient due to its tree structure and efficiency in accessing policy servers. The newest technology involved with directory services that works in conjunction with LDAP and is its possible replacement, is DSML. DSML is an application of the Extensible Markup Language (XML) and it enables different computer network directory formats to be expressed in a common format that can be shared by different directory systems.

Products

#	Application Authentication and Single Sign-On (SSO) Products
1.	**IBM Tivoli Access Manger** Provides a solution for securing web-based applications and can simplify application coding. Supports a variety of authentication techniques such as digital certificates and tokens without requiring any change on supported applications. Global Sign-on is an enterprise wide solution that also works with mainframe applications. Global Sign-on eases password management for users and improves security. Was previously called Tivoli Secureway Global Signon.

Tech Watch

• **Custom Web-Based Solution** – It may not be necessary to purchase a package solution to achieve single sign-on for web-based applications. A custom developed solution is feasible and, depending upon the enterprise requirements, can be more practical and cost effective when considering the costs of products that fall into the SSO category. Custom developed solutions take many shapes and forms and may include: secure and persistent cookies, secure HTTP header fields, Common ID, Password synchronization, SAML, Digital Certificates

• **Microsoft Passport & Liberty Alliance** - These two competing camps, organized by Microsoft and Sun, respectively, are currently developing a universal tool for allowing cross-platform and cross-application, cross-company, authentication and profile management for users. These two solutions are in their vision/formative stages and require significant product definitions, enhancements, and maturity over the near-term to be viable. Note, at this point, do not use either solution on systems requiring strong authentication, or those systems protecting sensitive information (these solutions have been known to introduce significant vulnerabilities).

Products to watch as potentially most suitable for use at the DMV are listed below:

- Web-based products for this category have been previously identified in the Authorization and Authentication Sub-Components

- Enterprise single sign-on solutions are more difficult to build, integrate, and deploy since they must interface with such a diverse set of back-end technologies including operating systems, network operating systems, mainframes, proprietary applications, and web-based applications. Potential solutions include

1. **Novell SecureLogin** - A directory enabled authentication solution that provides enterprise level single sign-on across a variety of platforms.
2. **Unisys e-@ction Single Sign On** - Provides both enterprise and web-based single sign-on in one package. This product provides the ability for an administrator to control access to workstations, back-end applications, and web-based applications. Unisys supports a variety of authentication mechanisms including user-ID/password, tokens, and biometrics.

Review Cycle

6 months

Application Controls

Definition

Application Controls are a part of application and systems development security that refer to the controls included within systems software and applications software, including the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

Development should follow a systems development life cycle (SDLC) and security must be considered in all phases. Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. It has long been a tenet of the security and development community that it cost ten times as much to add a feature in a system that has already been designed than to include the feature in the system at the initial design phase. Also, the principal reason for implementing security during a system's development is that it is more difficult to implement it later. It also tends to disrupt ongoing operations.

Security also needs to be incorporated into the later phases of the computer system life cycle to help ensure that security keeps up with changes in the system's environment, technology, procedures, and personnel. It also ensures that security is considered in system upgrades, including the purchase of new components or the design of new modules.

Life cycle management helps document security-relevant decisions, in addition to helping assure that management that security is fully considered during all phases of development.

Adding applications using open standards and common development practices allow for the secure creation of new applications. With ever-changing languages and data structures, using open industry standards will decrease the risks of development for the DMV.

Current and Future State

Current State	Future State
DMV currently using ENDEVOR to facilitate migration between environments for mainframe application development only. No methodology employed for any other development efforts.	The Department will need to embrace current development architectures that will allow for extensible and flexible development. E.g. J2EE, CORBA, RUP
Security personnel not directly involved in current application development efforts	Involve DMV security team in all future application development projects

Guidelines

#	Application Controls Guidelines
1.	Implement security considerations throughout the entire phase of the system development life cycle **Rationale**: • Following the SDLC model and its documentation, oversight and independent audit groups can verify that system management has done an adequate job and\or can highlight areas where security may have been overlooked.
2.	The costs related to standard security controls will be included as part of the Feasibility Study Report (FSR) for all new application proposals **Rationale**: • As the DMV will be adding security resources and features for all future application development efforts; this cost increase will need to be taken into account.
3.	The Department will employ its risk management methodology for all new or modified applications within the DMV environment. **Rationale**: • Risk management includes an overall security review; risk analysis, cost-benefit, and the selection, test, and implementation of security safeguards. This is a management and preventative technique used to control events that

	may introduce undesirable effects within the Department's systems. DMV systems will be developed according to its ISD Development Methodology plan.
4.	The DMV will establish a set of standards and a methodology for software development that incorporates security controls **Rationale**: • Considerable vulnerabilities and exposures are created in custom application environments. These vulnerabilities and exposures will go unchecked unless a standard process is in place for audit and verification. A standard methodology (and the use of a tool to effect the methodology) across the enterprise will position the DMV to mitigate risks and create a unified application environment to leverage best-practice security solutions for authentication, authorization, audit, and administration.

Standards

#	Application Controls Standards
1.	Utilize the BEAM Application Development component for implementation of security controls in all application development **Rationale**: • Current development standards provide the most stability, scalability and extensibility across the various vendor platforms and products: J2EE, JAAS, CORBA, Rapid Application Deployment (RAD), and Web Services. Object-oriented programming allows more efficient and faster development due to its inherent re-use of software modules.

Products

#	Application Controls Products
	No products are currently approved for use at the DMV within this Sub-Component.

Tech Watch

- **Web Services (UDDI, WSDL, SOAP)** is an immature but rapidly growing movement in the middleware and application development environment. It is XML-based and utilizes existing Internet technologies. Its aim is to provide a seamless layer of abstraction for eCommerce communication between organizations, while providing sufficient authorization and other security controls for users and their data. It also provides a means for service requestors to browse and locate services, as well as receive service descriptions directly from the service provider.

- **Rational Unified Process (RUP)** - The RUP methodology provides a recognized and widely adopted process for developing applications. RUP applies best practice software development techniques along with the application of the Unified Modeling Language (UML). RUP identifies a development process that incorporates “Inception”, “Elaboration”, “Construction”, and “Transition”, and with techniques for communication, collaboration, identifying development risks, establishing metrics, effective code re-use, and software testing. The widespread use of RUP within the DMV will by it’s very nature begin to mitigate risks associated with custom application development, such as ensuring a consistent set of application controls for authentication, authorization, audit, and administration.

- **Security Middleware -** The use of security “middleware” tools for messaging can help the Department position itself to tap the market as it matures. A market-leading product to monitor is Quadrasis Enterprise Application Security Integration (EASI) – (Quadrasis provides a security “middleware” tool for integrating security into EJB and CORBA environments. Quadrasis provides a solution for implementing security across the distributed enterprise and integrating a broad set of enterprise technologies. Quadrasis provides a critical layer of abstraction for integrating a variety of security point solutions and eliminating dependence on particular vendors. EASI is a necessary component to ensure uniformity across the enterprise and relies on messaging technologies such as SAML to deliver its capabilities. Quadrasis can be used to create a uniform security solution for the DMV’s messaging infrastructure.)

Review Cycle

6 months

Database Controls

**This section is addressed in the Decision Support component. Please refer to this section for policy and standards.

Testing Controls

**This section is addressed in the Testing component. Please refer to this section for policy and standards.

Revision History

June 22, 2000 – Component Principles version approved at Consensus Meeting.

December 20, 2001 – Products version approved at Consensus Meeting.

October 24, 2002 – Reviewed and approved for BEAM Intranet Site.

May 23, 2003 – add IBM OS/390 LDAP and IBM Tivoli Access Manager to Product lists.